VŠB – TECHNICKÁ UNIVERZITA OSTRAVA
Fakulta elektrotechniky a informatiky
Katedra elektroniky

Metody přenosu a zabezpečení dat pro aplikace v mobilních zařízeních

Disertační práce

Školitel: prof. Ing. Pavel Brandštetter, CSc.

Ostrava, duben 2011

Ing. Jan Vaněk

Prohlášení

Prohlašuji, že jsem tuto práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: Podpis:

Poděkování

Děkuji svému školiteli prof. Ing. Pavlu Brandštetterovi, CSc. a členům katedry elektroniky za cenné rady a odborné vedení v průběhu mého celého studia. Rovněž děkuji své rodině a přátelům za jejich trpělivost a podporu.

Anotace

Disertační práce se zabývá problematikou přenosu a zabezpečení dat pro aplikace v mobilních zařízeních. Po úvodu je proveden stručný popis použitých bezdrátových technologií. Jedná se konkrétně o GPRS, WiFi a Bluetooth. Následně je věnována pozornost seznámení s globálním pozičním systémem, který bude využit v aplikaci přenosu dat reprezentující spotřebu elektrické energie a polohu elektromobilu. V další části jsou uvedeny možnosti detekce a odstranění chyb při přenosu dat a také seznámení s asymetrickými a symetrickými šifrovacími metodami a implementačním popisem šifry AES. Poté je shrnuta bezpečnost bezdrátové komunikace a použitých přenosových technologií. Část práce tvoří návrh laboratorního pracoviště a mobilního systému, případně popis používaných hardwarových modulů. Stěžejní jsou experimentální výsledky, kde je ověřen šifrovaný i nešifrovaný přenos dat z mobilního systému s využitím předem popsaných bezdrátových technologií. Experimentální výsledky ukončuje aplikace monitorování spotřeby elektrické energie elektromobilu. V závěru jsou zhodnoceny přínosy a dosažené výsledky této práce.

Annotation

The dissertation deals with data transfer and security applications in mobile devices. After introduction, it is composed a description of wireless technologies. Specifically, it is GPRS, WiFi and Bluetooth Technologies. Subsequently, it is given attention to introduction of the global positional system which will be used in the application data transferring representing the power consumption and location electromobile. The next section describes the options for detection and removal errors data as well as familiarization with the asymmetric and symmetric encryption techniques and description of an implementation AES. Then it is summarized the safety of wireless communication and transmission technology. Part of this work consists of design of laboratory workplace, mobile systems and the description of hardware modules. Experimental results are pivotal and verify encrypted and unencrypted data transfer from a mobile system using pre-described wireless technology. Experimental results are rounded off by applications which monitor the power consumption of electromobile. Contributions and achievements of this work are in conclusion.

Obsah

Anotace **3**
Annotation **4**
Seznam použitých symbolů a zkratek **7**
Cíle disertační práce **9**
Úvod **10**
1 Bezdrátové přenosové technologie **11**
1.1 GPRS 11
1.1.1 Základní vlastnosti 11
1.2 WiFi 13
1.2.1 Dostupné rádiové frekvence 14
1.2.2 Struktura bezdrátové sítě 15
1.2.3 Přístupový bod 15
1.2.4 Ad-hoc sítě 15
1.2.5 Infrastrukturní sítě 16
1.3 Bluetooth 16
1.3.1 Popis systému 17
1.3.2 Struktura zařízení Bluetooth 17
1.3.3 Topologie systému 18
2 GPS **19**
2.1 Kosmický segment 19
2.2 Řídicí a kontrolní segment 19
2.3 Uživatelský segment 20
2.4 Rádiové signály 20
2.5 Souřadnicové systémy 21
2.6 Principy měření 21
2.7 Určování absolutní polohy 22
2.8 Standardy předávání dat 23
2.9 Faktory ovlivňující přesnost GPS 23
3 Detekce a odstranění chyb **24**
3.1 Kontrola opakováním 24
3.2 Kontrola parity 24
3.3 Podélná parita 25
3.4 Kontrolní součet 25
3.5 CRC 25
3.6 Oprava chyb 27
3.6.1 Jednotlivé potvrzování 27
3.6.2 Kontinuální potvrzování 28
3.6.3 Samostatné a nesamostatné potvrzování 28
4 Šifrování **29**
4.1 Symetrická kryptografie 29
4.1.1 Šifra AES 30
4.2 Asymetrické kryptografie 35

5 Bezpečnost bezdrátové komunikace 36
5.1 Zabezpečení GPRS 36
5.1.1 Autentizace 36
5.1.2 Šifrování 37
5.2 Zabezpečení Bluetooth 37
5.2.1 Inicializace 37
5.2.2 Autentizace 38
5.2.3 Šifrování 38
5.3 Zabezpečení WiFi 38
5.3.1 Obvyklé metody zabezpečení 39
6 Laboratorní pracoviště 40
6.1 Přenosové modely 40
6.2 Rozbor požadavků 41
6.3 Návrh mobilního systému 41
6.4 Hardwarové moduly 43
6.4.1 Kit eZdsp F28335 43
6.4.2 OEM RS232 Module Adapter III 44
6.4.3 Bluetooth rozšiřující deska 44
6.4.4 WiFi rozšiřující deska 45
6.4.5 GSM/GPRS rozšiřující deska 47
6.4.6 GPS modul 48
6.4.7 Elektroměr EM4T 51
7 Softwarové řešení 54
7.1 Systém se signálovým procesorem 54
7.2 Počítač pro sběr dat 55
8 Experimentální výsledky 57
8.1 Laboratorní pracoviště 57
8.2 Experimentální ověření přenosu dat 58
8.2.1 Přenos dat na PC prostřednictvím Bluetooth 58
8.2.2 Experimentální aplikace pro Pocket PC 62
8.2.3 Přenos dat prostřednictvím WiFi na FTP server 64
8.2.4 WiFi SerialNET 69
8.2.5 GSM SMS 72
8.2.6 Přenos dat z pracoviště pro bezsenzorové řízení asynchronních motorů 75
8.2.7 Monitorování spotřeby elektrické energie elektromobilu 80
9 Přínosy 88
Závěr 89
Použitá literatura 91
Publikace autora 94
Řešené grantové projekty 95

Seznam použitých zkratek a symbolů

Seznam zkratek

AES	-	Advanced Encryption Standard
AFH	-	Adaptive Frequency Hopping
AP	-	Access Point
ARP	-	Address Resolution Protocol
ARQ	-	Automatic Repeat reQuest
BTS	-	Base Transceiver Station
CAN	-	Controller Area Network
CRC	-	Cyclic Redundancy Check
CS	-	Code Scheme
DES	-	Data Encryption Standard
DHCP	-	Dynamic Host Configuration Protocol
DNS	-	Domain Name System
DSC	-	Digital Signal Controller
DSSS	-	Direct Sequence Spread Spectrum
ETSI	-	European Telecommunication Standards Institute
FHSS	-	Frequency Hopping – Spread Spectrum
EPC	-	Enhanced Power Control
FTP	-	File Transfer Protocol
GFSK	-	Gaussian Frequency-Shift Keying
GPRS	-	General Packet Radio Service
GSM	-	Global System for Mobile Communications
HLR	-	Home Location Register
HTTP	-	Hypertext Transfer Protocol
ICMP	-	Internet Control Message Protocol
IP	-	Internet Protocol
IMSI	-	International Mobile Subscriber Identify
LAN	-	Local Area Network
LSB	-	Least Significant Bit
MAC	-	Media Access Control
McBSP	-	Multichannel Buffered Serial Port
MCC	-	MobileCountry Code
MIME	-	Multipurpose Internet Mail Extensions
MIMO	-	Multiple Input, Multiple Output
MNC	-	Mobile Network Code
MSB	-	Most Significant Bit
NTP	-	Network Time Protocol

OFDM	-	Orthogonal Frequency Division Multiplexing
POP3	-	Post Office Protocol version 3
PSK	-	Phase Shift Keying
PWM	-	Pulse Width Modulation
RC4	-	Ron's Code 4
SCI	-	Serial Communication Interface
SIM	-	Subscriber Identity Module
SMTP	-	Simple Mail Transfer Protocol
SPI	-	Serial Peripheral Interface
SPP	-	Serial Port Profile
TCP	-	Transmission Control Protocol
TDD	-	Time Division Duplex
TDMA	-	Time Division Multiple Access
TELNET	-	Telecommunication Network
TMSI	-	Temporary Mobile Subscriber Identity
UDP	-	User Datagram Protocol
UTM	-	Universal Transverse Mercator coordinate system
WEP	-	Wired Equivalent Privacy
WGS-84	-	World Geodetic System 1984
WPA	-	WiFi Protected Access
802.1X	-	IEEE Standard for port-based Network Access Control

Seznam symbolů

$a_{x,y}$	-	bajt po operaci SubBytes
$c_{x,y}$	-	bajt po operace AddRoundKeys
$G(x)$	-	generující polynom
i	-	aktuální pozice slova
k	-	počet slov klíče
$k_{x,y}$	-	bajt podklíče
$M(x)$	-	vstupní polynom
$m_{x,y}$	-	bajt po operaci MixColumns
r	-	počet iterací
Rcon[i]	-	slovo označující výsledek po dělení
$R(x)$	-	polynom reprezentují zbytek po dělení
$s_{x,y}$	-	bajt po operaci ShiftRows
W	-	pole slov
w[i]	-	slovo v poli **W**

Cíle disertační práce

V rámci disertační práce jsou vytýčeny tyto cíle:

- Teoretický rozbor bezdrátových přenosových metod, jejich výhody a možnosti využití.
- Vytvoření přenosových modelů pro aplikace v mobilních zařízeních se zaměřením na bezdrátové technologie.
- Návrh a realizace laboratorního pracoviště pro experimentální ověření jednotlivých přenosových metod.
- Sestavení algoritmů a jejich implementace do řídicího přenosového systému se signálovým procesorem a do počítače určeného ke sběru dat.
- Experimentální ověření komunikace mezi řídicím systémem a počítačem určeným ke sběru dat.
- Teoretický rozbor symetrických a asymetrických šifrovacích metod a jejich porovnání.
- Optimalizace šifrovací metody pro jednotlivé přenosové metody.
- Sestavení šifrovacích algoritmů a jejich následná implementace.
- Experimentální ověření šifrovaného přenosu dat mezi řídicím systémem a počítačem určeným ke sběru dat.

Úvod

Vzhledem k tomu, že narůstá potřeba dohledu a komunikace s různými mobilními zařízeními, je nutné vypracovat metody, jak tyto požadavky řešit. Použití dnes běžných kabelových sítí není u mobilních zařízení zcela možné, nebo jen v omezeném rozsahu. Proto je vývoj věnován bezdrátovým technologiím. Je zřejmé, že o vhodnosti použití jednotlivých bezdrátových technologií rozhoduje celá řada faktorů. Mimo jiné akční rádius, vnější prostředí, četnost datových spojení, maximální přenosová rychlost, citlivost přenášených dat na zneužití a další. Právě zabezpečení přenášených dat proti zneužití je stále diskutovanější problematikou. Je to dáno mimo jiné tím, že se rádiový signál šíří i mimo předem vymezené prostředí, určené k pohybu zařízení, respektive jeho obsluhy. Pak již není velikým problémem odposlouchávání přenášených dat a jejich případné zneužití, pokud dojde k prolomení defaultních ochranných algoritmů. Na to lze však například reagovat nadstavbovým zabezpečením ještě před samotným odesláním dat.

Tato práce nejprve seznámí s použitými bezdrátovými technologiemi, konkrétně GPRS, WiFi a Bluetooth a naznačí jejich výhody. Dále bude uveden stručný popis GPS, který je následně využit v systému monitorování elektrické energie elektromobilu a sledování údajů o poloze, nadmořské výšce a podobně. Následně budou uvedeny metody detekce a odstraňování chyb a také podrobněji rozepsán CRC. V zápětí následuje obecný popis metod šifrování a implementační schéma symetrické iterační šifry AES. Také bude věnována pozornost bezpečnosti jednotlivých bezdrátových technologií. Před vytvořením laboratorního pracoviště je proveden rozbor požadavků na mobilní systém a další část pokračuje popisem navržených případně hotových hardwarových modulů. Samostatná kapitola seznámí se softwarovými prostředími určenými k programování DSC, případně pro komunikaci a nastavení hardwarových bloků. Stěžejní částí této práce budou experimentální výsledky, kde proběhne ověření jednotlivých přenosových metod a následná aplikace v systému monitorování spotřeby elektrické energie elektromobilu.

Využití se naskýtá v mnoha oborech elektroniky. Ať jde o vyčítání aktuální spotřebované energie z vozidel s elektrickou trakcí a její následné vizualizace, nebo přenos dat mezi subsystémy, které není možné z různých důvodů propojit kabelovým systémem.

1 Bezdrátové přenosové technologie

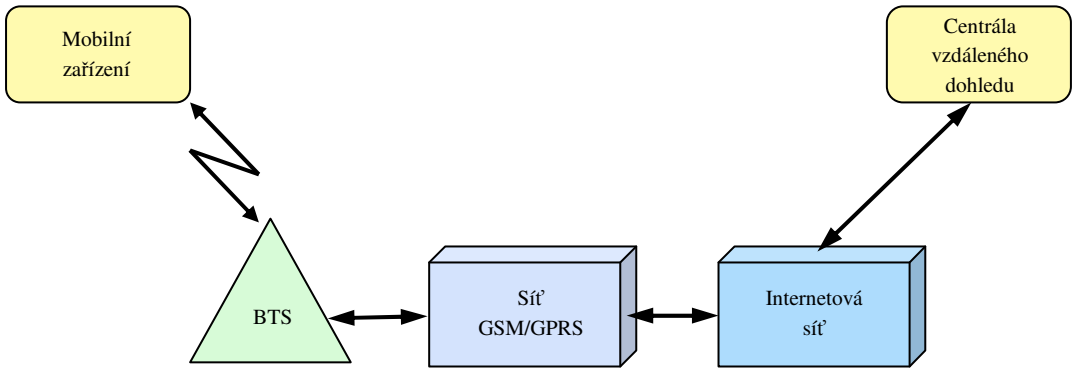
Bezdrátové přenosové technologie disponují zásadní výhodou v trvalém dohledu nad mobilními zařízeními. Ať se již jedná o přenos povozních údajů, nebo provádění dozoru a řízení. Technicky je možné bezdrátové technologie rozdělit dle jejich přenosové vzdálenosti. Každá aplikace má konkrétní požadavky na oblast pokrytí signálem vzhledem k rádiusu svého pohybu. V dalším textu jsou popsány základní dostupné přenosové technologie s různým pokrytím a od toho odvíjející se akční rádius.

1.1 GPRS

GPRS neboli General Packet Radio Services je mobilní technologie, která pracuje na tzv. paketovém přenosu dat, umožňující dynamickou změnu přenosové rychlosti pro uživatele. Využívá stávající sítě GSM, která v případě České republiky pokrývá cca 98% území. Umožňuje připojení založené na internetových protokolech, které podporují širokou škálu podnikových a obchodních aplikací. K přenosu dat mezi mobilními uživateli a sítí je použito rádiových a síťových zdrojů dostupných na požádání. Data jsou rozdělena do paketů a poté přenesena přes rádiovou síť a páteřní sítě. Nevýhodou je relativně velká latence (kolem 500 ms) a nepříliš vysoká přenosová rychlost. V následujícím textu o GPRS je čerpáno z [1], [2], [3].

1.1.1 Základní vlastnosti

GPRS umožňuje rychlé spojení, kterým mohou být informace rozesílány neprodleně v případě potřeby, avšak nutnou podmínkou pro dostupnost je rádiové pokrytí GSM. Rychlost spojení je dána tím, že více uživatelů GPRS sdílí identický přenosový kanál a jsou stále připojeni. Pak je celková kapacita vyhrazena uživatelům posílajícím nebo přijímajícím data. Sdílením datové kapacity je docíleno vyšší datové propustnosti v situacích, kdy uživatelé občasně odesílají nebo přijímají data. GPRS umožňuje mnoho možností využití, jako je prohlížení webových stránek, využívání internetových aplikací, přenos souborů mezi mobilním zařízením, také možnost vzdáleného přístupu a kontroly, případně monitorování objektu, zařízení nebo stroje. Na obrázku 1.1 je zjednodušená struktura přenosu dat sítí.



Obrázek 1.1 Zjednodušená struktura přenosu dat

Se současnými i budoucími mobilními datovými sítěmi je technologie GPRS naprosto kompatibilní. Důvodem fyzického a praktického vzdálení se síti GSM je to, že síť GPRS využívá hlavně rádiovou část a přibližuje se spíše datovým sítím a oblastem informačních technologií.

Systém kódování	Přenosová rychlost [kbit·s^{-1}]	Uživatelská rychlost [kbit·s^{-1}]
CS1	9,1	6,7
CS2	13,4	10,0
CS3	15,6	12,7
CS4	21,4	16,7

Tabulka 1.1 Systémy kódování a jejich rychlosti

ETSI specifikovala pro kódování na rádiovém rozhraní čtyři kódovací systémy CS a v tabulce 1.1 jsou jejich přenosové rychlosti. Kódovací systém CS1 představuje nejbezpečnější způsob kódování s vysokou odolností proti chybám na rádiovém rozhraní. Nízká výsledná přenosová rychlost je dána velkou redundancí kódu. Při využití kódovacího systému CS4 je naopak výsledná přenosová rychlost mnohem vyšší, ale tento systém je pak z pohledu odolnosti proti chybám nejméně odolný. V závislosti na dostupnosti sítě, kanálu a kódovacím systému nabízí GPRS až teoretických $21{,}4 \cdot 8 = 171{,}2$ kbit·s^{-1}. Toto zvýšení rychlosti je dosaženo použitím všech osmi timeslotů rámce TDMA a kódovacího systému CS4. Výběr kódovacího systému provádí systém a nelze jej během přenosu jednoho datového bloku měnit.

Třída	Rx	Tx	Maximální počet timeslotů
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
5	2	2	4
6	3	2	4
7	3	3	4
8	4	1	5
9	3	2	5
10	4	2	5
11	4	3	5
12	4	4	5

Tabulka 1.2 Třídy GPRS

Charakteristika rozdělení dostupných timeslotů se však může v čase lišit. To je zapříčiněno komutací paketů. Navíc je z pohledu uživatele výhodnější uvažovat tzv. uživatelskou rychlost. Ta je vždy nižší, poněvadž je uvažován přenos dodatečných informací přenosových protokolů fyzické vrstvy. Uživatelskou rychlost pro kódovací systém CS4 je

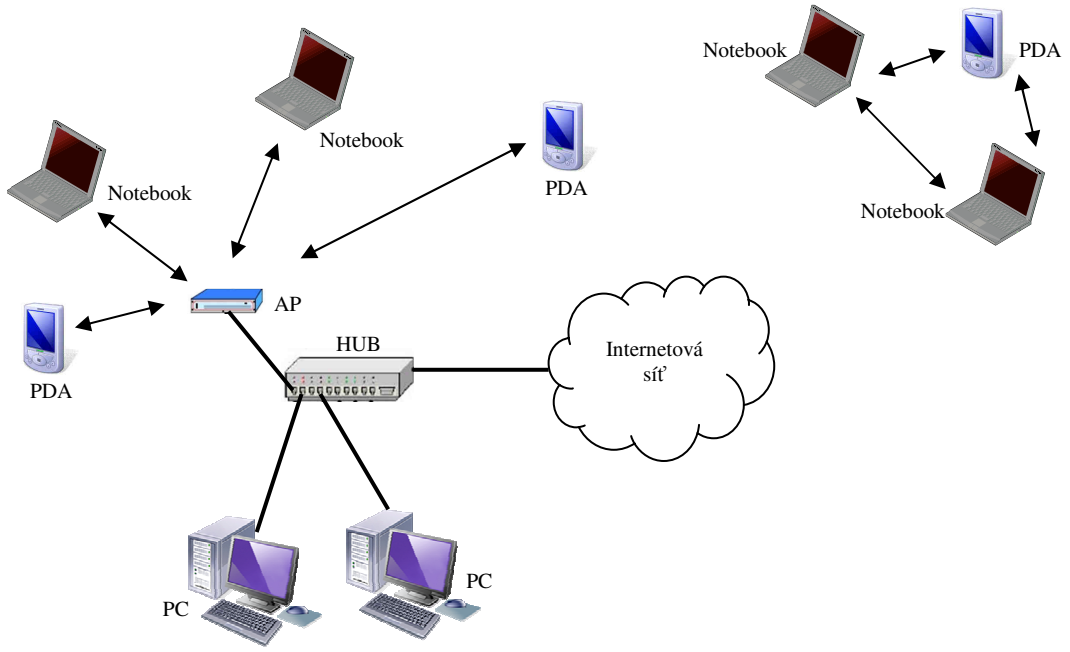
možno stanovit na 16,7 · 8 = 133,6 kbit·s^{-1}. Výsledná uživatelská rychlost bude v důsledku využití dalších protokolů, např. IP, ještě menší.

Variabilita systému GPRS umožňuje konfiguraci parametrů sítě a počtu použitých timeslotů pro uplink a downlink. Základní rozdělení mobilních zařízení do tříd podle počtu timeslotů je naznačeno v tabulce 1.2. Přidělení konkrétního počtu timeslotů závisí na konfiguraci jednotlivých buněk.

Na kvalitu přenášeného signálu má největší vliv rádiové prostředí. Tento vliv je mnohem větší než u metalických nebo optických kabelů. Tedy rychlost přenosu v GPRS bude záviset na úrovni rušení v síti. Pak pro kódovací systémy CS3 a CS4 může docházet k opakování přenosů chybně přijatých paketů dat v prostředí s vyšším rušením.

1.2 WiFi

WiFi je standard pro lokální bezdrátové sítě (Wireless LAN, WLAN) a vychází ze specifikace IEEE 802.11. Původním cílem WiFi sítí bylo zajišťovat vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální (např. firemní) sítě LAN viz obrázek 1.2. S postupem času začala být využívána i k bezdrátovému připojení do sítě Internet v rámci rozsáhlejších lokalit a tzv. hotspotů. WiFi zařízení jsou dnes prakticky ve všech přenosných počítačích a i v některých mobilních telefonech. Úspěch WiFi přineslo využívání bezlicenčního pásma, což má negativní důsledky ve formě silného zarušení příslušného frekvenčního spektra a dále častých bezpečnostních incidentů [4].



Obrázek 1.2 Přístupová metoda sítí 802.11

1.2.1 Dostupné rádiové frekvence

V tabulce 1.3 je uveden přehled standardů IEEE 802.11, jejich rádiové pásmo, maximální rychlost a také přenosová technika použitá na fyzické vrstvě [5].

- **DSSS** (Direkt Sequence Spread Spektrum) je technika přímého rozprostřeného spektra. Jedná se o to, že jednotlivé bity určené k přenosu jsou nahrazeny sekvencí bitů, mající obvykle pseudonáhodný charakter. Tato sekvence bitů je pak modulována na nosný signál. Tím je uměle zavedena redundance. Takovýto signál je pak méně citlivý vůči rušení. Signál se pak jeví jako náhodný šum a bez znalosti mechanizmu vytvoření původní pseudonáhodné sekvence může být obtížné získat přenášená data [19].

- **OFDM** (Ortogonal Frequency Division Multiplex) je technika pracující s rozprostřeným spektrem a signál se vysílá na více nezávislých frekvencích. Datový tok celého kanálu se dělí na mnoho dílčích datových toků jednotlivých nosných. Na přijímací straně je možné přijmout právě vysílaný symbol, přestože přichází k přijímači různými cestami s různým zpožděním. To má za následek zvýšení odolnosti vůči interferencím.

- **MIMO** (Multiple Input Multiple Output) využívá vícecestné komunikace u multi-anténních komunikačních systémů, mající za následek zvýšení propustnosti datového kanálu. Výhodou je také zvýšení dosahu a snížení bitové chybovosti. Obecně tato technologie zefektivňuje spektrální účinnost rádiových systémů [6], [19].

Standard	Pásmo [GHz]	Maximální rychlost [Mbit·s^{-1}]	Fyzická vrstva
IEEE 802.11	2,4	2	DSSS
IEEE 802.11a	5	54	OFDM
IEEE 802.11b	2,4	11	DSSS
IEEE 802.11g	2,4	54	OFDM
IEEE 802.11n	2,4 nebo 5	600*	OFDM, MIMO

Tabulka 1.3 Přehled standartů IEEE 802.11

* 802.11n – ve fázi Draft 2.0 dle návrhu od skupiny TGn sync bude rychlost až 600 Mbit·s^{-1} při 4X4 MIMO (4 streamy), až 450 Mbit·s^{-1} při 3X3 MIMO (příklad implementace: Intel® WiFi Link 5300 Series), až 300 Mbit·s^{-1} při 2X2 MIMO (např.: Intel® WiFi Link 5100 Series). 802.11n – Skutečná rychlost při 600 Mbit·s^{-1} na fyzické vrstvě (L1) je údajně až do 400 Mbit·s^{-1} na MAC (L2 - Layer2 - MAC) vrstvě. Praktická rychlost bude nižší. Intel® WiFi Link 5100 v noteboocích běžně zvládá reálné rychlosti nad 100 Mbit·s^{-1} [5].

1.2.2 Struktura bezdrátové sítě

Bezdrátová síť může být vybudována různými způsoby v závislosti na požadované funkci. Ve všech případech hraje klíčovou roli identifikátor SSID (Service Set Identifier), což je řetězec až 32 ASCII znaků, kterými se jednotlivé sítě rozlišují. SSID je jedinečný identifikátor každé bezdrátové (WiFi) počítačové sítě. Přístupový bod (AP) vysílá pravidelně každých několik sekund svůj identifikátor v takzvaném majákovém rámci (Beacon Frame) a klienti si tak mohou snadno zobrazit dostupné sítě a vybrat, ke které bezdrátové síti se připojí (tzv. asociovat se s přístupovým bodem) [7].

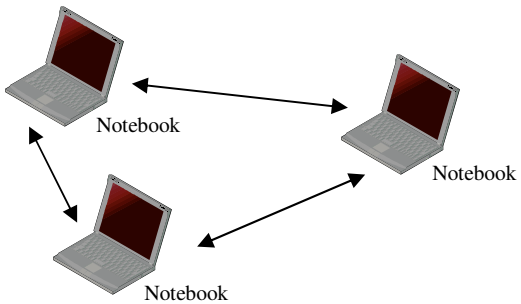
1.2.3 Přístupový bod

Přístupový bod představuje přemostění mezi kabelovou a bezdrátovou sítí, přestože poskytuje i celou řadu dalších funkcí. Klienti spolu komunikují prostřednictvím AP, čímž mezi sebou nemusejí být ve vzájemném rádiovém spojení. Centralizovaný způsob komunikace navíc umožňuje využívání směrových antén a tím zvětšení dosahu rádiového signálu. Tento způsob komunikace je nazýván jako infrastrukturní síť. Opakem je Ad-hoc síť, u nichž jsou dva nebo více klientů v přímém rádiovém spojení bez existence prostředníka.

Realizace přístupového bodu je obvykle řešena malým jednoúčelovým zařízením, nicméně s potřebnou softwarovou výbavou se jím může stát i jakýkoli počítač s bezdrátovým WiFi zařízením.

1.2.4 Ad-hoc sítě

Sítě Ad-hoc se někdy nazývají nezávislé sítě, z toho důvodu, že jednotlivé stanice spolu komunikují přímo, nezávisle na nějakém prostředníkovi. Vzájemná identifikace probíhá pomocí SSID. Pokud spolu stanice chtějí komunikovat, musí být ve vzájemném dosahu. To je typické pro malou síť, kde jsou jednotlivé stanice vzdáleny od sebe jen několik metrů. Na obrázku 1.3 je znázorněno vhodné komunikační schéma. Je jasné, že v místech, kde princip vzájemného rádiového dosahu nemůže být zajištěn, pak toto komunikační schéma realizovat nelze. Nezávislé sítě Ad-hoc nedoznaly větší obliby nejen z důvodu omezené rozlehlosti sítě, ale také proto, že jejich nárazové vytvoření vyžaduje nakonfigurování sítě a to laický uživatel ne vždy zvládne [8].

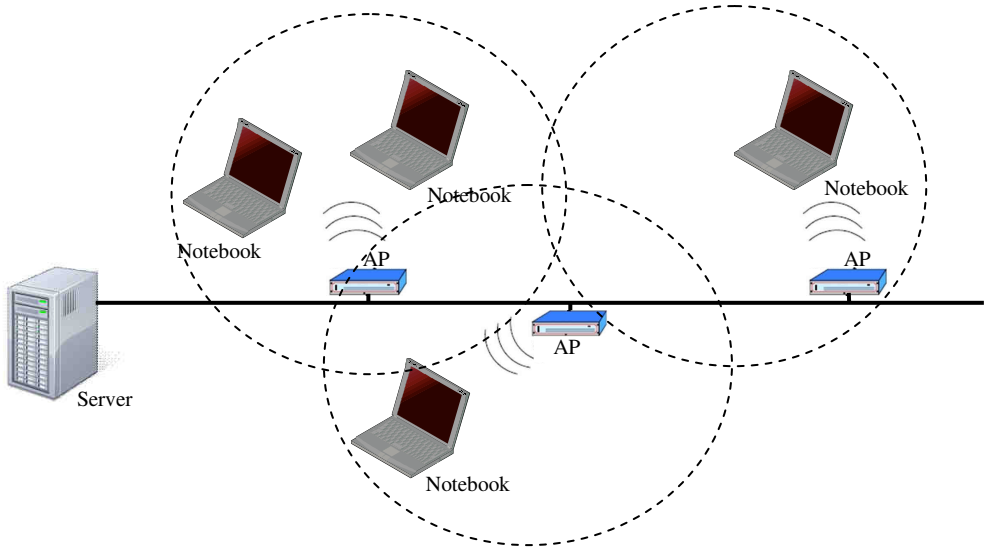


Obrázek 1.3 Síť Ad-hoc

1.2.5 Infrastrukturní sítě

Název infrastrukturní sítě plyne z toho, že je přesně dána jejich infrastruktura. Roli spojovacího článků přijímají přístupové body, které vysílají své SSID (obrázek 1.4). Přístupový bod zde plní funkci datového mostu (bridge).

Přístupový bod je schopen komunikovat s více než jednou stanicí a proto může propojovat i bezdrátové stanice, jež se nalézají v jeho dosahu a nezávisle na tom, zda-li tyto stanice chtějí používat most do kabelového Ethernetu.



Obrázek 1.4 Infrastrukturní síť

Další možností je, že bude mít několik AP stejné SSID a pak plně záleží na klientovi, ke kterému AP se připojí. Volba pak může záviset na síle signálu a tak umožňovat klientovi volný pohyb ve větší síti (tzv. roaming).

Asociace stanice s přístupovým bodem je v infrastrukturní síti nutná. Bez toho je vytvoření sítě nemožné. Asociační proces vždy inicializuje mobilní stanice a AP připojení k sobě buď odmítne anebo mobilní stanici k sobě připojí. Stanice nemůže být asociována k více přístupovým bodům současně [8].

1.3 Bluetooth

Systém Bluetooth je univerzální radiokomunikační systém, umožňující bezdrátový přenos datových signálů s přenosovou rychlostí až 24 Mbit·s^{-1} ve verzi 4.0. Je použitelný na krátké vzdálenosti (do desítek metrů). Umožňuje bezdrátově propojit různá elektronická zařízení, například počítač, řídicí systém, senzorové subsystémy aj. Tím dochází k odstranění propojení pomocí metalických kabelů, které nemusí být v určitých aplikacích vhodné nebo žádoucí. Další informace vycházejí z [1], [10], [11], [12], [13].

1.3.1 Popis systému

Bluetooth pracuje v bezlicenčním pásmu 2,4 GHz (Industrial-Scientific-Media band, ISM), konkrétně v rozsahu 2,400 GHz – 2,4835 GHz a využívá digitální modulaci GFSK. Použití frekvenčního skoku s rozprostřeným spektrem (FHSS) má za cíl snížení rušení mezi technologiemi pracujícími ve spektru 2,4 GHz. To má za následek vysoký stupeň imunity vůči rušení a umožnění efektivního přenosu ve spektru. Ve vytvořené pikosíti udává pořadí frekvencí Master a následně je pokračováno v pseudonáhodném pořadí, čímž je zajištěno, že v každé pikosíti budou jiné hodnoty frekvencí. Takto je možno provozovat co možná největší počet nezávislých pikosítí v malém prostoru. Při metodě kmitočtových skoků je použita rychlost 1600 skoků za sekundu. Zařízení Slave mají k začátku vysílání poskytnutou časovou prodlevu 625 μs od zařízení Master. Tyto prodlevy jsou počítány v závislosti na hodinách zařízení Master. K zajištění obousměrného provozu je použita metoda TDD a Master může zahájit přenos dat pouze na začátku sudé časové prodlevy a zařízení Slave naopak liché časové prodlevy.

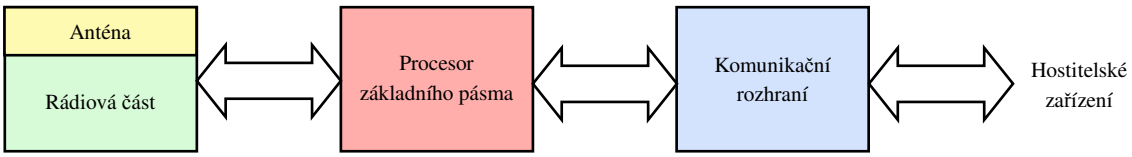
U verze 2.0 standardu Bluetooth je rozšířená metoda kmitočtových skoků o AFH, kdy zařízení Master může v pikobuňce zařízením Slave zadávat používané a nepoužívané frekvence. Rychlost přenosu dat je až 3 $Mb \cdot s^{-1}$.

Verze Bluetooth 3.0 využívá protokolu 802.11 PAL, což znamená, že přenos dat může probíhat i přes WiFi, pakliže jsou oba spárované přístroje touto technologií vybaveny. Maximální rychlost je udávána na 24 $Mb \cdot s^{-1}$ a samozřejmostí je také kompatibilita se staršími verzemi. Také je implementována technologie EPC, snižující spotřebu elektrické energie a omezující množství výpadků při přenosu dat na minimum.

V nové verzi Bluetooth 4.0, která se objevila v roce 2011, výrobci slibují menší energetickou náročnost, podporu šifrování AES-128, avšak maximální rychlost 24 $Mb \cdot s^{-1}$, nadále zůstává stejná jako v předchozí verzi.

1.3.2 Struktura zařízení Bluetooth

Součástí každé sítě jsou tedy elektronická zařízení obsahující rádiovou část tvořenou bezdrátovým vysílačem a přijímačem, procesorem základního pásma a komunikačním rozhraním. Na obrázku 1.5 je blokové schéma zařízení Bluetooth. Procesor základního pásma komunikuje prostřednictvím komunikačního rozhraní s hostitelským systémem, dále řídí činnost rádiové části a v neposlední řadě i komunikaci v síti.



Obrázek 1.5 Blokové schéma zařízení Bluetooth

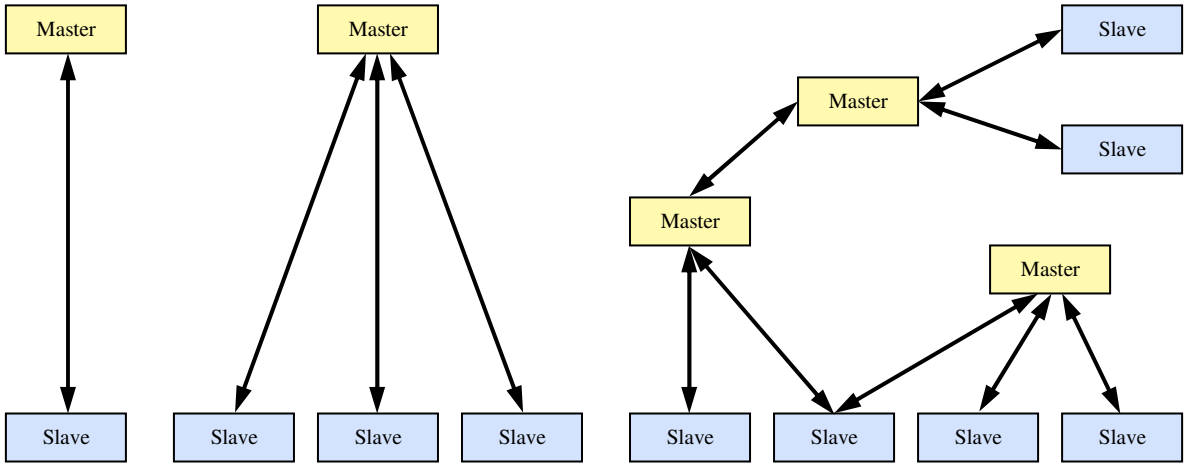
Provozní dosah závisí na třídě zařízení, jak ukazuje tabulka 1.4. Nízko energetické technologie Bluetooth mají dosah až 200 m nebo 600 m.

Třída rádia 3	Dosah až 1 m	Výkonová úroveň 2,5 mW
Třída rádia 2	Dosah až 10 m (mobilní zařízení)	Výkonová úroveň 10 mW
Třída rádia 1	Dosah až 100 m (průmyslové použití)	Výkonová úroveň 100 mW

Tabulka 1.4 Dosah v závislosti na třídě rádia a výkonu vysílače

1.3.3 Topologie systému

Základní topologie sítě se skládá z malých struktur s názvem pikonet. Síť Bluetooth využívá principu Master-Slave, kde Master řídí tok dat. Na obrázku 1.6 jsou rozlišeny následující typy sítí Bluetooth.



Obrázek 1.6 Typy sítí Bluetooth a) Pikosíť Point to Point, b) Multi Slave, c) Scatternet

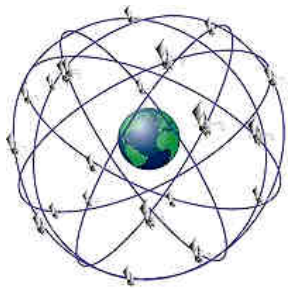
- **Režim Mono Slave** nastává, pokud bude navzájem propojen Master s jedním zařízením typu Slave a jde-li o připojení Point-to-Point (obrázek 1.6 a).
- **Režim Multi Slave,** kde může být připojeno až sedm zařízení Slave pomocí připojení Point-to-Multipoint (obrázek 1.6 b). Všechny stanice jsou vzájemně rovnocenné a spojení funguje bez hierarchické struktury, pouze terminál, jež sestavoval spojení je označen jako Master a ostatní zařízení jsou onačena jako Slave. Master inicializuje vytváření sítě, identifikuje účastníky, řídí synchronizaci a podobně. Tyto funkce však trvají pouze po dobu spojení.
- Takzvaný **Scatternet** vzniká spojením několika pikosítí. Protože je v každé pikosíti právě jeden Maser, bude nyní situace taková, že zařízení pracující v jedné síti jako Master, může být v jiné síti jako Slave. Scatternet sítě se však do dnešních aplikačních rodin protokolů Bluetooth neprosadily.

2 GPS

Mobilní systémy, potažmo uživatelé mobilních systémů, stále častěji vyžadují informace o aktuální poloze. Nejde jen o nutnost tarifikace trakčních vozidel, nebo kontrolu aktuální polohy, ale také o sledování členitosti terénu a informace o nadmořské výšce a podobně. Je to dáno potřebou kontroly a dohledu nad pohybujícími se zařízeními. Pro potřeby navigace a určování polohy na zemi je vybudován globální polohový systém (GPS). Je zde však jedna omezující podmínka použitelnosti a to je přímá viditelnost na oblohu. Systémy GPS tedy není možné používat v budovách, pod velmi hustou vegetací a podobně. V dalším textu o GPS je vycházeno z [14], [15], [16]. Jsou popsány tři základní segmenty, tvořící systém GPS, což je kosmický, řídicí a kontrolní a uživatelský. Následně je věnována pozornost použitým rádiovým signálům, principům měření a zjednodušenému popisu GPS.

2.1 Kosmický segment

Na oběžných drahách je vytvořena soustava družic, vysílajících navigační signály. Původně byl projektován na 24 družic, ale současné době obsahuje mezní počet 32. Oběžné dráhy mají stálou polohu vůči zemi. Doba oběhu družic je přibližně 12 hodin. Původní konstelaci tvoří šest oběžných drah se čtyřmi družicemi na každé z nich (obrázek 2.1). Nyní je na každé oběžné dráze 5–6 nepravidelně rozmístěných družic. Sklon oběžné dráhy je přibližně 55 stupňů vzhledem k rovníku. Tato konfigurace garantuje minimální dostupnost signálu ze čtyř družic.



Obrázek 2.1 Rozmístění družic

V Česku je nejčetnější viditelnost osmi družic, minimum pak 6 a maximum 12 družic. Dlouhodobá stabilita systému je zajištěna díky kruhové oběžné dráze a relativně velké oběžné výšce (20200 km). Družice jsou několikrát do roka, obvykle plánovaně, odstaveny pro údržbu atomových hodin a korekci dráhy družice. Průměrná životnost družice je zhruba 10 let.

2.2 Řídicí a kontrolní segment

Řídicí a kontrolní segment monitoruje kosmický segment, zasílá povely družicím, provádí údržbu atomových hodin, umožňuje ovládání družic a je zodpovědný za řízení celého globálního polohovacího systému. Tvoří jej soustava pěti monitorovacích stanic, tří stanic pro komunikaci s družicemi a hlavní řídicí stanice.

Pozemní monitorovací stanice jsou dálkově řízeny z hlaví řídicí stanice. Jedná se o velice přesné GPS přijímače, doplněné o vlastní atomové hodiny. Umožňují sledování aktuálně viditelných družic a přenášejí informace hlavní řídicí stanici, která vypočítává přesné údaje oběžných drah a korekce atomových hodin jednotlivých družic. Ty jsou dále přeneseny na stanice pro komunikaci s družicemi a minimálně jednou denně odesílány na jednotlivé družice.

2.3 Uživatelský segment

Uživatelský segment tvoří uživatelé, GPS přijímače, vyhodnocovací nástroje a postupy. Výpočty rychlosti, polohy a času jsou provedeny GPS přijímači na základě signálů z družic. Všechny čtyři souřadnice (x, y, z, t) jsou vypočítány po příjmu signálu minimálně od čtyř družic. Využití GPS přijímačů může být následující:

- Určení polohy.
- Určování přesného času.
- Určování rychlosti.
- Určení nadmořské výšky.
- Určení azimutu pohybu.
- Navigace ve třírozměrném prostoru a další.

2.4 Rádiové signály

Signály vysílané družicemi GPS jsou kombinací nosné vlny, dálkoměrného kódu a navigační zprávy. Při tvorbě vysílaného signálu se vychází z toho, že jednotlivé složky jsou odvozeny násobením a dělením základní frekvence.

Družice vysílají signály na dvou nosných frekvencích. Frekvence L1 (1575,42 MHz) a L2 (1227,6 MHz).

- **L1** je modulována dvěma dálkoměrnými kódy. Ty jsou reprezentovány pseudonáhodnými šumy. Značí se jako signály standardní polohové služby.

  Jde o přesný P-kód, jež může být zašifrován pro vojenské účely a pak se značí jako Y-kód. Jedná se o pseudonáhodný kód, jehož celková délka je přibližně 266 dnů. Je rozdělen na sedmidenní sekvence a každé družici je přidělena jedna z nich. Rovnice pro dekódování P-kódu jsou všeobecně známé, zatímco pro Y-kód jsou utajeny a znají je pouze autorizovaní uživatelé.

  Dále je dostupný C/A kód, který není šifrovaný. Jedná se v podstatě o posloupnost 1023 nul a jedniček, která je svým charakterem blízká šumu, je jednoznačně definována. Každá stanice má přidělen svůj vlastní C/A kód a rovnice pro jeho dekódování jsou všeobecně známé. Většina civilních přijímačů využívá pouze C/A kód.

- **L2** je modulována jen P-kódem, resp. Y-kódem. Využívá se pro přesnou polohovou službu.

Dále je mezi oběma nosnými frekvencemi přenášen ještě binární kód, jehož obsahem je navigační zpráva. Obsahuje přesnou polohu družice v době odesílání dálkoměrného kódu. Poloha se počítá na základě parametrů dráhy družice. Navigační zpráva obsahuje nejen parametry oběžné dráhy dané družice, ale i další informace, jako například čas vysílání počátku zprávy, údaje umožňující přesně korigovat čas vysílání družice, koeficienty ionosférického modelu a další. Na základě těchto údajů je tedy možné spočítat přesnou polohu družice a přesný čas odesílání přijaté sekvence dálkoměrného kódu.

Provozovatel GPS má možnost kdykoli snížit přesnost systému. Je k tomu využita takzvaná selektivní dostupnost. Ta sníží přesnost C/A kódu a výpočet polohy pak může obsahovat chybu až 100 m. Tuto chybu je však možno eliminovat dalšími metodami.

2.5 Souřadnicové systémy

Pro určování polohy jsou definovány základní souřadnicové systémy. Vzhledem k tomu, že systém GPS tvoří 3 základní segmenty, z nichž jeden je umístěn ve vesmíru a zbylé dva na Zemi, musí GPS pracovat vnitřně se dvěma typy souřadnicových systémů.

GPS pracuje s geocentrickými souřadnicemi spojenými se zemským tělesem. Ty jsou vhodné pro oba pozemní segmenty. Nicméně pro popis pohybu družic je výhodnější systém, jehož střed je umístěnce středu sluneční soustavy. Vzhledem k tomu, že provozovatel systému řeší transformace mezi těmito systémy, uživatele GPS se tyto problémy netýkají.

Podstatné je, že GPS přijímače poskytují polohu v geografických souřadnicích vztažených ke Světovému geodetickému systému WGS-84. Navíc v případě potřeby je možný převod do některého běžného kartografického zobrazení.

2.6 Principy měření

Pro určování polohy a času jsou využity tři základní principy měření. Jedná se konkrétně o kódová, fázová a Dopplerovská měření.

- **Kódová měření** představují základní princip měření pomocí systému GPS. Jakmile se na vstupu přijímače objeví signál z jedné družice, je přijímaná nosná vlna L1, jež je modulována kódem C/A, převedena na signál nižší frekvence a následně směšována s C/A kódem generovaným v přijímači, který ovšem není synchronní s C/A kódem vysílaným družicí. Je to dáno menší stabilitou hodin v přijímači a časovým posunem mezi odesláním družicí a příjmem přijímačem. Nyní přijímač hledá pro neznámou družici odpovídající dálkoměrný kód a postupným posunem přijímačem generované sekvence se snaží dosáhnout shody obou signálů. Po synchronizaci je dosaženo vyrušení obou C/A kódů a je k dispozici pouze nosná vlna modulována navigační zprávou. Protože družice vysílá jednotlivé sekvence C/A kódu v přesně stanovené

okamžiky, je možné pomocí C/A kódu a navigační zprávy určit přesný čas odeslání signálu. Rozdíl mezi časem odeslání sekvence C/A kódu a časem jejího přijetí přijímačem pak odpovídá době šíření signálu od družice k přijímači. Následně se vypočítá vynásobením rychlostí šířením vln zdánlivá vzdálenost přijímače od družice. Tato vzdálenost je však zatížena určitou chybou danou mnohem nižší přesností hodin v přijímači. V případě měření pomocí P-kódu je postup podobný.

- **Fázová měření** nepracují s dálkoměrnými kódy, ale zpracovávají vlastní nosné vlny. Dá se říci, že přijímač spočítá počet vlnových délek mezi vysílačem a přijímačem nosné vlny. Ten je dán celočíselným násobkem nosných vln a desetinou částí. Nastává problém, že u klasické sinusové vlny nelze určit čas jejího odeslání, jako je to možné u dálkoměrných kódů. Proto vzniká nejednoznačnost týkající se počtu celých vlnových délek nosné vlny, jež se nachází mezi přijímačem a družicí. Tedy přesně je přijímač schopen určit jen tu část vlny vyjádřenou jako úhel mezi 0 a 360°. Byly vypracovány postupy umožňující řešit tento problém a to buď v reálném čase anebo při následném zpracování.

- **Dopplerovská měření** využívají Dopplerův posun. Vzhledem k tomu, že poloha družice vůči přijímači se stále mění, je možno sledováním frekvence nosné vlny zjistit frekvenční posun. Frekvenční posun je určitou dobu měřen a dle získaných údajů je pak umožněn výpočet změny radiální vzdálenosti mezi přijímačem a družicí. Poloha přijímače pak může být vypočtena z rozdílů těchto vzdáleností.

2.7 Určování absolutní polohy

Absolutní poloha může být určena pomocí zdánlivých vzdáleností, které jsou získány z kódových měření.

Pokud jsou hodiny přijímače i družice synchronní a neexistují další vlivy způsobující náhodné změny výsledků, pak z jednoho měření zdánlivé vzdálenosti určíme, že přijímač se nachází na kulové ploše se středem v družici a poloměrem rovným vypočtené vzdálenosti. Jestliže současně provedeme stejné měření vzhledem k druhé družici, zjistíme, že se obě kulové plochy protínají v kružnici a přijímač se tedy nachází někde na této kružnici. Třetí současně změřená vzdálenost jiné družice pak definuje další kulovou plochu, která se s kružnicí protne ve dvou bodech, z nichž jeden můžeme vyloučit, jelikož leží daleko ve vesmíru. Čili současné měření vzdáleností ke třem družicím nám teoreticky poskytne přesnou polohu v třírozměrném prostoru.

Vzhledem k částečné nesynchronnosti hodin času družice a přijímače, se systémovým časem družicového polohovacího systému je potřeba postup určování absolutní polohy přizpůsobit. Je možné dodatečně korigovat časové údaje družic vzhledem k časovému posunu systémového času, ale časový posun hodin přijímače ΔT vůči systémovému času je stále neznámý. To se projeví na jednotlivých vzdálenostech tak, že jednotlivé vzdálenosti se budou

lišit o vzdálenost, kterou urazí rádiové vlny za ΔT. Pak již průsečíkem není bod, ale po převedení do roviny trojúhelník. Řešením je provedení ještě jednoho měření, kdy jsou měřeny zdánlivé vzdálenosti přijímače ke čtyřem družicím, což vede k soustavě čtyř rovnic o čtyřech neznámých, s tím že v každé rovnici figuruje ΔT. Poloha je pak vypočtena v geocentrických souřadnicích a obvykle pak bývá převedena do souřadnic geografických.

2.8 Standardy předávání dat

Standardy umožňují vzájemnou datovou komunikaci mezi přijímači a dalšími systémy. Pro komunikaci mezi dvěma přijímači v diferenčním módu vznikl standard RTCM SC-104. Dále pro výstupní data existuje standard RINEX a NMEA.

RTCM SC-104 definuje přenos diferenčních korekcí pro uživatele GPS. Je definován binární formát předávání dat. Základní blok je rámec, který se skládá z 30ti bitových slov. Každé slovo obsahuje jeden nebo několik parametrů. Datové informace jsou obsaženy v prvních 24 bitech a zbývajících 6 je použito pro zabezpečení a detekci chyb.

RINEX je využíván pro komunikaci mezi GPS přijímači a nadřazeným systémem. Popisuje textový formát, kde délka řádku je z důvodu usnadnění prohlížení na obrazovce omezena na max. 80 znaků. Jsou definovány tři typy souborů a to soubor obsahující naměřená data, dále soubor obsahující navigační zprávy a konečně soubor obsahující meteorologická data.

NMEA 0183 je specifikován pro komunikaci mezi námořními elektronickými zařízeními, jako jsou sonary, anemometry, kompasy, autopiloty, GPS přijímače atd. a definuje sériovou asynchronní komunikaci mezi zdrojem dat a nadřazeným systémem. Komunikace probíhá v textovém módu prostřednictvím ASCII znaků. V jedné větě může být obsaženo až 82 znaků. Tento standard je využíván přijímačem Garmin viz kapitola 6.4.6, kde je podrobněji rozebrán.

2.9 Faktory ovlivňující přesnost GPS

Přesnost polohy určená přijímačem GPS se může pohybovat v širokých mezích. Dále jsou uvedeny faktory, mající na přesnost určování polohy a času vliv.

- Řízení přístupu k signálům z družic.
- Počet viditelných družic
- Rozsah přesnosti měření.
- Vícecestné šíření.
- Geometrické uspořádání viditelných družic.
- Chyba hodin přijímače.
- Způsob měření a vyhodnocování a další.

3 Detekce a odstranění chyb

Při přenosu dat může docházet k chybám, způsobeným různými faktory. Mohou nastat chyby v případě úplného výpadku spojení, nebo chyby náhodné, kde vlivem rušení dojde k záměně přenášených informací. Pokud nejsou tyto chyby detekovány a přijímač je nerozpozná, dochází k výraznému ovlivnění informační hodnoty zprávy a často i k výpadku funkce zařízení, které je na těchto informacích závislé. V dalším textu jsou uvedeny základní metody detekce chyb a způsoby získání správných dat. Již nyní je jasné, že všechny metody sebou přinášejí jistou redundanci při přenosu dat, protože k přenášeným informačním datům přidávají určité množství kontrolních bitů. Existují detekční kódy, jež umožňují pouze rozpoznat, že přijatý blok dat je chybný a dále samoopavné kódy, zvládající chybu nejen najít, ale také opravit, čímž odpadá nutnost data posílat znovu.

V praxi bývá výhodné nezabezpečovat vůči chybám jednotlivé bajty, nýbrž celé posloupnosti bajtů. Pak se dodatečné detekční bity přidávají až na konec posloupnosti dat. Jestliže je chyba detekována, nelze ji v bloku lokalizovat a je nutné zaslání celého bloku dat znova, což celkově nevadí, protože data jsou posílána po blocích a selekce chybných dat by zabrala leckdy více času, než poslání celého bloku. Dále je čerpáno z [17], [18], [19], [23].

3.1 Kontrola opakováním

Existuje mnoho variací na opakovací schéma a všechny jsou založeny na tom, že posílaná data jsou rozdělena do bloků stejné délky a každý blok je odeslán několikrát za sebou. Využívá se lichého počtu opakování. Jakmile jsou bloky ekvivalentních dat přijaty a jsou všechny stejné, je možno tvrdit, že v přenosu nenastala chyba. Chyba se dá také najít a s určitou pravděpodobností odstranit v případě přijetí ekvivalentních bloků dat, z nichž většina je stejná a ta pak může být brána za správnou hodnotu. Problém nastává u chyb projevujících se ve stejném okamžiku, kdy ekvivalentní posílaná data jsou vlivem chyby změněna na stejném místě. Pak se data jeví jako bezchybná a informace o vzniklé chybě je takto potlačena. Toto schéma tedy není přes svou jednoduchost příliš výkonné a nemůže být použito po data s vyšší prioritou.

3.2 Kontrola parity

Jedna ze základních detekčních metod, využívaných převážně u asynchronních přenosů je kontrola parity. Je to nejjednodušší, ale zároveň nejméně účinný způsob, jak doplněním jednoho bitu k přenášenému bloku dat, tyto data zabezpečit a následně rozpoznat chybu. V případě sudé parity je doplněním paritního bitu celkový počet jedniček ve vysílaném bloku sudý, kdežto u liché parity lichý. Příjemce pak musí být informován o použití sudé nebo liché parity.

Jestliže počet jedničkových bitů nesouhlasí s očekávanou paritou, pak došlo k chybě jednoho respektive obecně lichého počtu bitů. Avšak i když má přijatá zpráva očekávanou

paritu, neznamená to, že je zcela jistě přijata správně. Pomocí jediného paritního bitu tedy nelze rozpoznat chyby v sudém počtu bitů. Použití tohoto zabezpečení je vhodné v případech, kde pravděpodobnost výskytu chyb v jednotlivých bitech je malá a pravděpodobnost výskytu chyb ve více bitech je současně zanedbatelná.

3.3 Podélná parita

Celý blok dat, chápaný jako posloupnost bajtů, je možno zabezpečit podélnou paritou. Zde není kontrolován počet sudých nebo lichých bitů v jednotlivých bajtech, ale počet sudých nebo lichých jedničkových bitů na stejných bitových pozicích jednotlivých bajtů. Blok dat je tvořen jednotlivými bajty a tedy je přidáno k celému bloku bajtů dalších osm paritních bitů viz obrázek 3.1.

Bajt 1	1	1	0	1	0	1	1	1
Bajt 2	1	1	1	1	1	1	1	1
Bajt 3	0	1	0	1	0	1	0	1
Bajt 4	1	1	0	1	1	1	0	0
Bajt 5	1	1	1	0	1	1	0	0
Podélná parita	0	1	0	0	1	1	0	1

Obrázek 3.1 Naznačení příkladu sudé podélné parity

Použití podélné parity se někdy kombinuje se zabezpečením jednotlivých bajtů pomocí sudé nebo liché parity, která se pak označuje jako příčná nebo znaková parita.

3.4 Kontrolní součet

Je další možností zabezpečení celého bloku dat. Provádí se součtem jednotlivých bajtů v bloku dat a bajty jsou chápány jako celá dvojková čísla bez znaménka. Typicky je prováděn součet modulo 2^8 nebo 2^{16}. Výsledkem je pak kontrolní součet o délce jednoho nebo dvou bajtů.

3.5 CRC

Cyclic Redundancy Check představuje nejúčinnější formu zabezpečení bloku dat. Jedná se o cyklický kód. CRC typicky přidává k datovému bloku 8 až 32 kontrolních bitů, což v závislosti na generujícím polynomu, použitém algoritmu a počtu kontrolních bitů dává téměř 100% pravděpodobnost odhalení chyby. Kontrola probíhá tak, že příjemce dat opět vypočte CRC a porovná s přijatou kontrolní částí. Pokud se oba cyklické kontrolní součty rovnají, příjemce prohlásí data za správná.

CRC metoda nakládá se vstupním blokem dat jako s polynomem. Bit na posici LSB je přirovnán ke koeficientu x^0 polynomu, další bit vlevo ke koeficientu x^1 atd. To je znázorněno na obrázku 3.2, kde konkrétní binární data (101001101) jsou reprezentována koeficienty polynomu *M(x)*.

Obrázek 3.2 Reprezentace jednotlivých koeficientů u binárních dat

Pak polynom *M(x)* vypadá následovně:

$$M(x) = x^8 + x^6 + x^3 + x^2 + 1 \tag{3.1}$$

Obecně výpočet CRC probíhá dělením vstupního polynomu *M(x)* generujícím polynomem *G(x)* s tím, že výsledný podíl nebude použit a jako výsledek slouží zbytek po dělení *R(x)*. Polynom *R(x)* je následně interpretován jako bitová posloupnost, která se připojí za přenášená data reprezentovaná bitovou posloupností respektive polynomem *M(x)*. Při vhodně zvoleném generujícím polynomu *G(x)* vede i malá změna ve vstupní posloupnosti k podstatně odlišnému výsledku *R(x)*. Pravděpodobnost odhalení chyby výrazně roste se stupněm *G(x)*.

Generující polynom je průmyslem přijatá bitová posloupnost pro použití v CRC. Některé běžné generující polynomy jsou uvedeny v tabulce 3.1.

CRC-12	$G(x)=x^{12}+x^{11}+x^3+x^2+x+1$
CRC-16	$G(x)=x^{16}+x^{15}+x^2+1$
CRC-CCITT	$G(x)=x16+x^{15}+x^5+1$
CRC-32	$G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$
ATM CRC	$G(x)=x^8+x^2+x+1$

Tabulka 3.1 Běžně používané generující polynomy

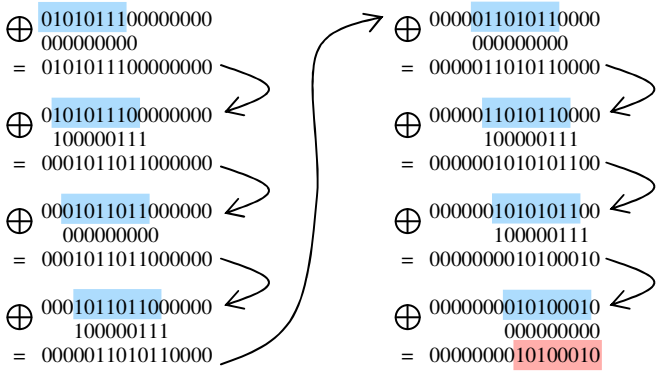
Na obrázku 3.3 je znázorněn příklad postupu tvorby *R(x)*. Vstupní data jsou reprezentována ASCII hodnotou písmena "W", jehož hexadecimální zápis je 57. Pokud bude LSB první vpravo, binární posloupnost je 01010111 a *M(x)* vypadá následovně:

$$M(x) = x^6 + x^4 + x^2 + x + 1 \tag{3.2}$$

Jako generující polynom bude použit (3.3) jehož binární posloupnost je 100000111.

$$G(x) = x^8 + x^2 + x + 1 \tag{3.3}$$

Před startem výpočtu je potřeba *M(x)* doplnit zprava počtem nulových bitů rovným se stupněm polynomu *G(x)*, v tomto případě 8. Po každém kroku dochází k posunu modrého okna doprava.



Obrázek 3.3 Naznačený příklad výpočtu CRC

Pokud je na posici MSB v modrém okně 0, pak se provede XOR s 000000000, jinak s 100000111. Výsledkem je zbytek označený červeně, jež reprezentuje CRC.

CRC je velice výkonná technika vyhledávání chyb a může být využita ve všech přenosových systémech. Například lokální počítačové sítě využívají CRC-32, Internet používá CRC-16 a mnoho dalších přenosových sítí má implementováno CRC a to nejen z důvodu jednoduchosti a snadné hardwarové i softwarové implementace, ale hlavně pro jeho prakticky 100% pravděpodobnost odhalení chyby.

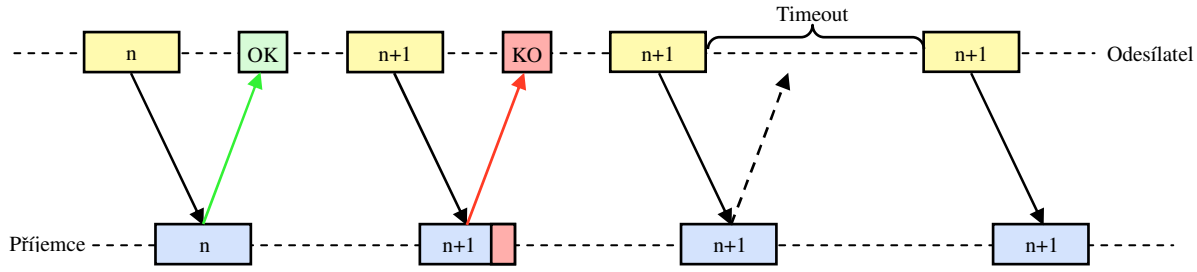
3.6 Oprava chyb

Jakmile jsou chybná data detekována, musí být použit nějaký mechanismus, pro opravu chyb. V předchozím textu byly popsány základní mechanismy detekce chyb, i když například CRC umí v jisté míře chyby i opravit. Je jasné, že existují samoopravné kódy zabezpečující přenášená data a v případě výskytu určitého počtu chyb je dokáží opravit například Hammingův kód. Samoopravné kódy však mají podstatnou nevýhodu v mnohem větší přenosové náročnosti, protože aby dokázaly opravit byť jen malé množství chyb, vyžadují přenos velkého množství redundantních dat, nutných pro případnou opravu poškozených informací. Jsou využívány převážně v situacích absence zpětného potvrzovacího kanálu mezi přijímačem a vysílačem, nebo v situacích, kdy nepřipadá v úvahu opětovné poslání dat.

Z praktického hlediska bude nyní věnována pozornost metodám, zajišťující komunikaci mezi přijímačem a vysílačem v rámci odstranění chyb celého bloku dat. Nutnou podmínkou aby se odesílatel dozvěděl, zda byla data na straně příjemce v pořádku, či nikoli je existence zpětného přenosového kanálu mezi přijímačem a vysílačem. Tato zpětná vazba pak určí, zda celý blok dat opakovat, nebo ne a existuje v několika variantách.

3.6.1 Jednotlivé potvrzování

Neboli také Stop-and-wait ARQ je technika, kdy odesílatel odešle blok dat a nejprve čeká na odezvu z druhé strany. Jestliže je odezva kladná, pokračuje v odesílání dalšího bloku dat. Pokud je však odezva záporná, odešle stejný blok znovu. Je však nutno počítat s dalšími možnostmi. Buď se mohl ztratit celý přenášený blok dat, čímž příjemce neví, že by měl cokoli potvrdit anebo se ztratilo samotné potvrzení generované příjemcem.



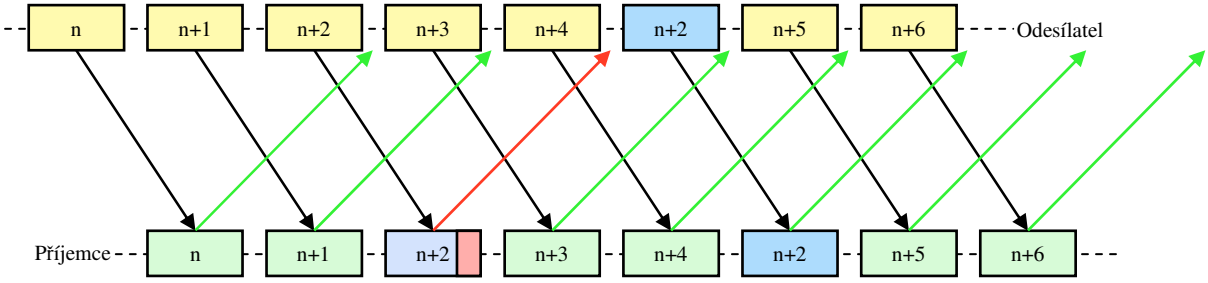
Obrázek 3.4 Příklad jednotlivého potvrzování

Vysílací strana musí počkat určitou dobu (anglicky Timeout) a pokud v tomto čase nedostane žádné potvrzení, zopakuje přenos dat. Obrázek 3.4 představuje příklad jednotlivého

potvrzování. Je jasné, že časový limit je potřeba volit pečlivě, aby nebyl přenos předčasně vyhodnocen jako chybný, nebo aby se zbytečně přenos nezpomaloval. Tato technika je vhodná tam, kde není velké přenosové zpoždění, hlavně v lokálních sítích a podobně. Jinak neúměrně narůstají prodlevy způsobené čekáním na potvrzení jednotlivých bloků.

3.6.2 Kontinuální potvrzování

Rozdíl oproti jednotlivému potvrzování je v tom, že odesílatel nečeká na jednotlivá potvrzení a pokračuje odesíláním dalších bloků dat. Data jsou tedy odesílána za sebou a odesílatel zpětně přijímá informace o tom, jak byly bloky dat doručeny. Obrázek 3.5 ilustruje princip kontinuálního odesílání se selektivním opakováním. Černé šipky značí odesílaní dat a zelené a červená potvrzování. Blok n+2 byl vyhodnocen jako blok s chybou a červenou šipkou je vyžádán opakovaný přenos bloku, který však nastane až po odeslání bloku n+4. Nevýhodu tvoří vyšší paměťové nároky na příjemce, který musí data průběžně přijímat a ukládat bez zpracování do paměti, dokud nepřijme znovu správná data, která předtím byla poškozena.



Obrázek 3.5 Příklad kontinuálního potvrzování se selektivním opakováním

Tento problém je možno vyřešit pomocí metody zvané opakování s návratem. Změnou oproti selektivnímu opakování je, že jakmile odesílatel dostane informaci o chybně přijatém bloku dat (nebo vyprší časový limit), znovu odešle příslušný blok dat a pokračuje bloky po něm následujícími, bez ohledu na to, že již mohly být odeslány. I přes svou šetrnost k příjemci má však tato metoda nevýhodu v odesílání bloků, které byly už jednou správně přijaty, čili snižuje přenosovou kapacitu.

3.6.3 Samostatné a nesamostatné potvrzování

Samotná potvrzení vysílaná k odesílateli dat musí mít svou konkrétní podobu. V případě samostatného potvrzování jde principielně o podobné bloky, jakými se přenášejí samotná data. Čili jedná se o bloky mající mimo jiné kontrolní část, hlavičku a podobně. Toto samozřejmě zvyšuje nároky na přenos.

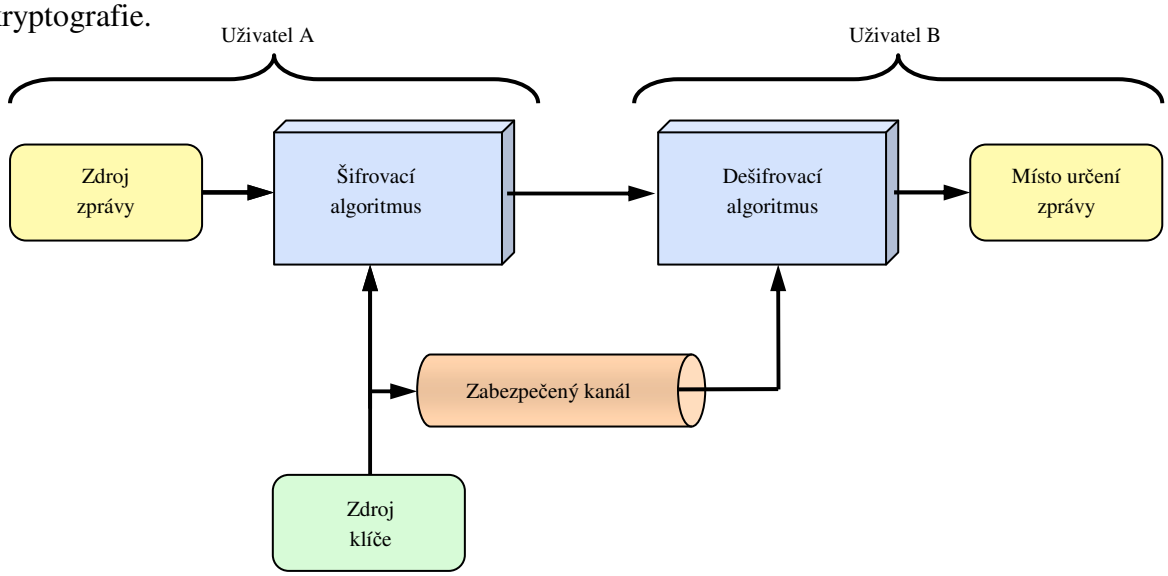
U nesamostatného potvrzování je snaha ušetřit přenosové prostředky tím, že potvrzovací data se přidají do bloku užitečných dat směřujícího k odesílateli původních dat. Je tedy využito zpětného toku dat z jiného přenosu a tím je ušetřena režie na přenos hlavičky a dalších náležitostí. Ovšem problém nastává v tom, že příjemce nemůže čekat příliš dlouho, až budou v opačném směru přenášena data k „vysílači“, čímž by mohl vypršet časový limit (Timeout). V praxi, se příjemce pokouší o nesamostatné potvrzení jen určitou dobu, a pokud se nepodaří nesamostatné potvrzení, je následně odesláno samostatné potvrzení.

4 Šifrování

Kryptografie respektive šifrování je věda o metodách, pomocí nichž dochází k utajování smyslu zpráv, tak že jsou převedeny do podoby, čitelné pouze se znalostí tajného klíče. S tímto pojmem se lze také obecně setkat u popisu metod spojených se šiframi jako alternativou k pojmu kryptologie. Kryptologie tedy zahrnuje kryptografii a kryptoanalýzu, neboli dešifrování zašifrovaných zpráv.

4.1 Symetrická kryptografie

Pokud je pro šifrování a dešifrování zprávy používán jediný klíč, hovoří se o symetrické, respektive konvenční kryptografii. To je také rozdílem od algoritmů s veřejným klíčem, které používají dvojici klíčů, tajný a veřejný. Hlavní výhodou symetrických šifer je jejich relativně nízká výpočetní náročnost na rozdíl od algoritmů pro šifrování s veřejným klíčem, jež můžou být i stotisíckrát pomalejší. Zásadní nevýhodou je však nutnost sdílení tajného klíče. To sebou přináší problémy s distribucí tajných klíčů mezi odesílatelem a příjemcem. Z tohoto důvodu se soukromý klíč často mění. Variantou u specifických zařízení je bezpečné uložení soukromého klíče přímo v zařízení [20], [21]. Obrázek 4.1 ukazuje princip symetrické kryptografie.



Obrázek 4.1 Princip symetrické kryptografie

Jak již bylo zmíněno, je častým případem použití symetrických šifer společně s asymetrickými. Obvykle se obou metod používá tak, že se otevřený text zašifruje symetrickou šifrou s náhodně vygenerovaným symetrickým klíčem a následně je tento klíč zašifrován veřejným klíčem asymetrické šifry. Dešifrovat data pak může pouze majitel tajného klíče dané asymetrické šifry [22].

Symetrické šifry se mohou rozdělit na proudové (FISH, RC4), které zpracovávají otevřený text po jednotlivých bitech, nebo blokové (DES, AES), které nejprve rozdělí otevřený text na bloky definované velikosti a následně tyto bloky zašifrují jako celek [23].

4.1.1 Šifra AES

Bloková šifra AES je nástupcem dříve hojně používaného šifrovacího algoritmu DES, který byl využíván pro šifrování neklasifikovaných dat ve federálních institucích USA a jehož krátká délka klíče dovolovala zaútočit na DES hrubou silou. Informace v dalším textu jsou čerpány z [24], [25], [26], [27], [28].

AES je iterační šifra s délkou bloku 128 bitů, kde počet iterací je závislý na délce klíče. Pro délky klíče 128, 192 a 256 bitů je počet iterací základní transformace 10, 12, 14. AES stejně jako podobné iterační šifry, vytváří ze šifrovacího klíče několik podklíčů, které se pak používají v jednotlivých iteračních cyklech. Nešifrovaný nebo šifrovaný text je reprezentovaný jako dvojrozměrné pole bajtů 4x4. Na obrázku 4.2 je znázorněno uspořádání bajtů v dvourozměrném poli.

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Obrázek 4.2 Uspořádání bajtů v dvourozměrném poli

AES transformuje blok otevřeného textu s využitím čtyř operací:

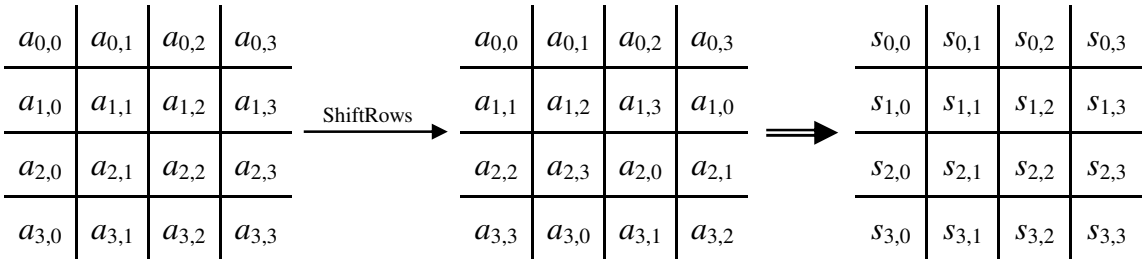
- **SubBytes** (substituce bajtů). Každý bajt pole je nahrazen novým bajtem dle předem daného algoritmu Rijndael-S-Box. Tím je zajištěna nelineárnost šifry, která zabraňuje útokům založeným na jednoduchých algebraických výpočtech.

	x0	**x1**	**x2**	**x3**	**x4**	**x5**	**x6**	**x7**	**x8**	**x9**	**xA**	**xB**	**xC**	**xD**	**xE**	**xF**
0x	63	7C	77	7B	F2	6B	6F	5C	30	01	67	2B	FE	D7	AB	76
1x	CA	82	9C	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2x	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3x	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4x	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5x	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6x	E0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7x	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8x	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9x	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
Ax	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
Bx	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
Cx	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
Dx	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
Ex	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
Fx	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tabulka 4.1 Rijndael-S-Box reprezentovaný hexadecimálně

Řádky tabulky 4.1 prezentují nejvíce významné 4 bity a sloupce nejméně významné 4 bity. Například vstupní bajt bude **9A**, pak výstupní bajt bude v devátém řádku a sloupci A, čili **B8**.

- **ShiftRows** (cyklický posun řádků pole). Každý řádek je posunut doleva o různý počet bajtů s tím, že první řádek se neposouvá a další řádky postupně o jeden, dva, tři bajty doleva viz obrázek 4.3.

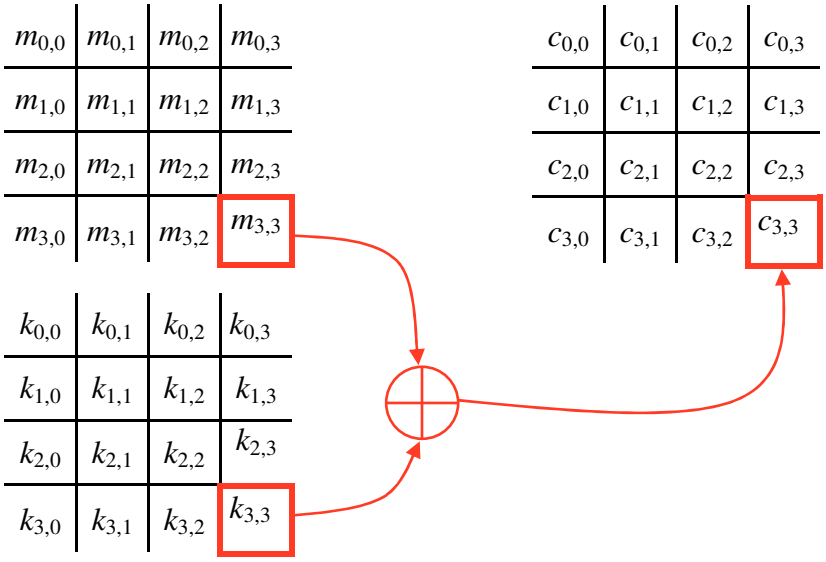


Obrázek 4.3 Cyklický posun řádků pole

- **MixColumns** (transformace sloupců algoritmu). Každý sloupec se nahradí novým sloupcem dle předpisu (5.1), kde je operace násobení pro implementaci definována jako: násobení 1 znamená opuštění beze změny, násobení 2 je bráno jako rotace bajtu vlevo a násobení 3 je řešeno rotací bajtu vlevo a provedením XOR s počáteční hodnotou.

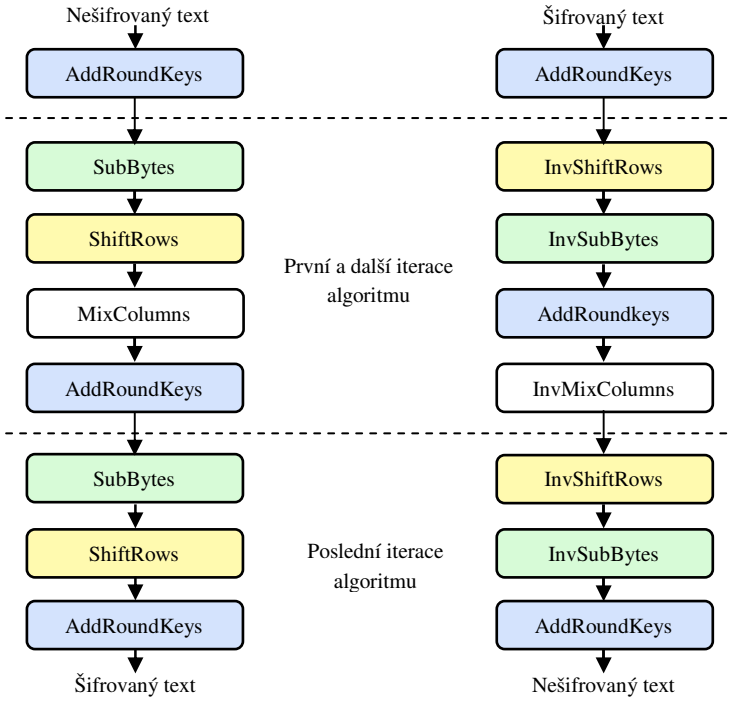
$$\begin{bmatrix} m_{0,n} \\ m_{1,n} \\ m_{2,n} \\ m_{3,n} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} s_{0,n} \\ s_{1,n} \\ s_{2,n} \\ s_{3,n} \end{bmatrix} \tag{4.1}$$

- **AddRoundKeys** (přičtení podklíče k poli). Pole podklíče má velikost 16 bajtů a sčítání je realizováno pomocí XOR odpovídajících bajtů podklíče a bajtů pole viz obrázek 4.4.



Obrázek 4.4 Sčítání odpovídajících bajtů pole a podklíče

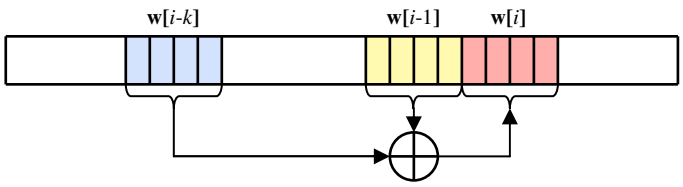
Všechna kola algoritmu jsou sestavena ze stejné posloupnosti operací, s výjimkou prvního kola, kde se navíc vkládá AddRoundKey a posledního kola, kde se vynechá operace MixColumns. Na obrázku 4.5 je ukázán algoritmus šifrování a dešifrování.



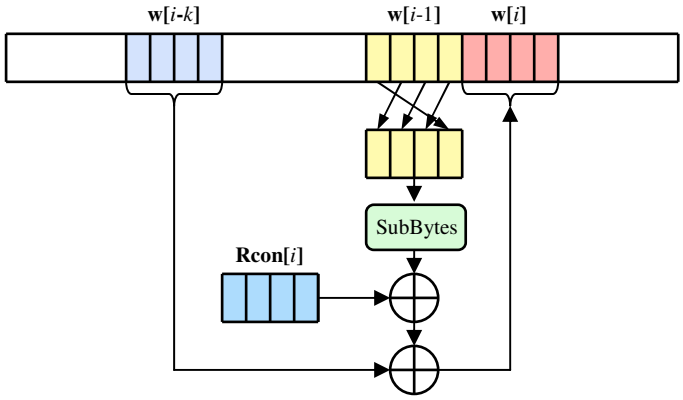
Obrázek 4.5 Naznačení šifrovacího a dešifrovacího algoritmu

Při vytváření podklíčů je nutno zohlednit variabilní délku klíče, různý počet iterací a tedy i různý počet podklíčů. Slovem se u AES značí posloupnost čtyř bajtů a ty jsou také základními jednotkami, s nimiž pracuje algoritmus pro tvorbu podklíčů. Tento algoritmus vytváří dostatečně dlouhé pole slov **W** a podklíče jsou brány z tohoto pole. Pole musí obsahovat $4 \cdot r$ slov, kde r značí počet iterací.

Pro délky klíče 128, 192 a 256 bitů je pak počet slov k klíče postupně roven 4, 6 a 8. Začátek pole **W** se naplní šifrovacím klíčem. Další slova v poli **W**, označené **w[***i***]** se vypočítají pomocí XOR slov **w[***i*-1] a **w[***i*-*k***]**. Pokud je aktuální pozice slova i dělitelná k, tak ještě před operací XOR se provede transformace slova **w[***i*-1**].** Transformace se skládá z rotace bajtů slova o jeden bajt doprava a substituce každého bajtu ve slově pomocí Rijndael-S-Box a následného XOR s konstantou **Rcon[***i***]**. Nakonec je proveden XOR se slovem **w[***i*-*k***].** Slovo **Rcon[***i***]** je výsledkem po dělení pozice slova i počtem slov k klíče a provedenou rotací o jeden bajt doprava. Na obrázku 4.6 a 4.7 je znázorněn schematický výpočet pole **W**.



Obrázek 4.6 Schematický výpočet pole **W** bez užití transformace slova **w[***i*-1**]**



Obrázek 4.7 Schematický výpočet pole **W** s použitím transformace slova **w[***i*-1**]**

K dešifrování textu se využívají inverzní operace k těm, které byly použity při šifrování s výjimkou AddRoundKey, kde přičtením stejného podklíče jako při šifrování se podklíč vyruší. Pořadí podklíče při dešifrování je opačné než při šifrování. Dešifrování je naznačeno na obrázku 4.5.

- **InvSubBytes** je inverzní funkce k funkci SubBytes. Je využit inverzní Rijndael-S-Box viz tabulka 4.2.

	x0	**x1**	**x2**	**x3**	**x4**	**x5**	**x6**	**x7**	**x8**	**x9**	**xA**	**xB**	**xC**	**xD**	**xE**	**xF**
0x	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1x	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2x	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3x	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4x	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5x	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6x	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7x	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8x	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9x	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
Ax	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
Bx	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
Cx	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
Dx	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
Ex	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
Fx	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Tabulka 4.2 Inverzní Rijndael-S-Box reprezentovaný hexadecimálně

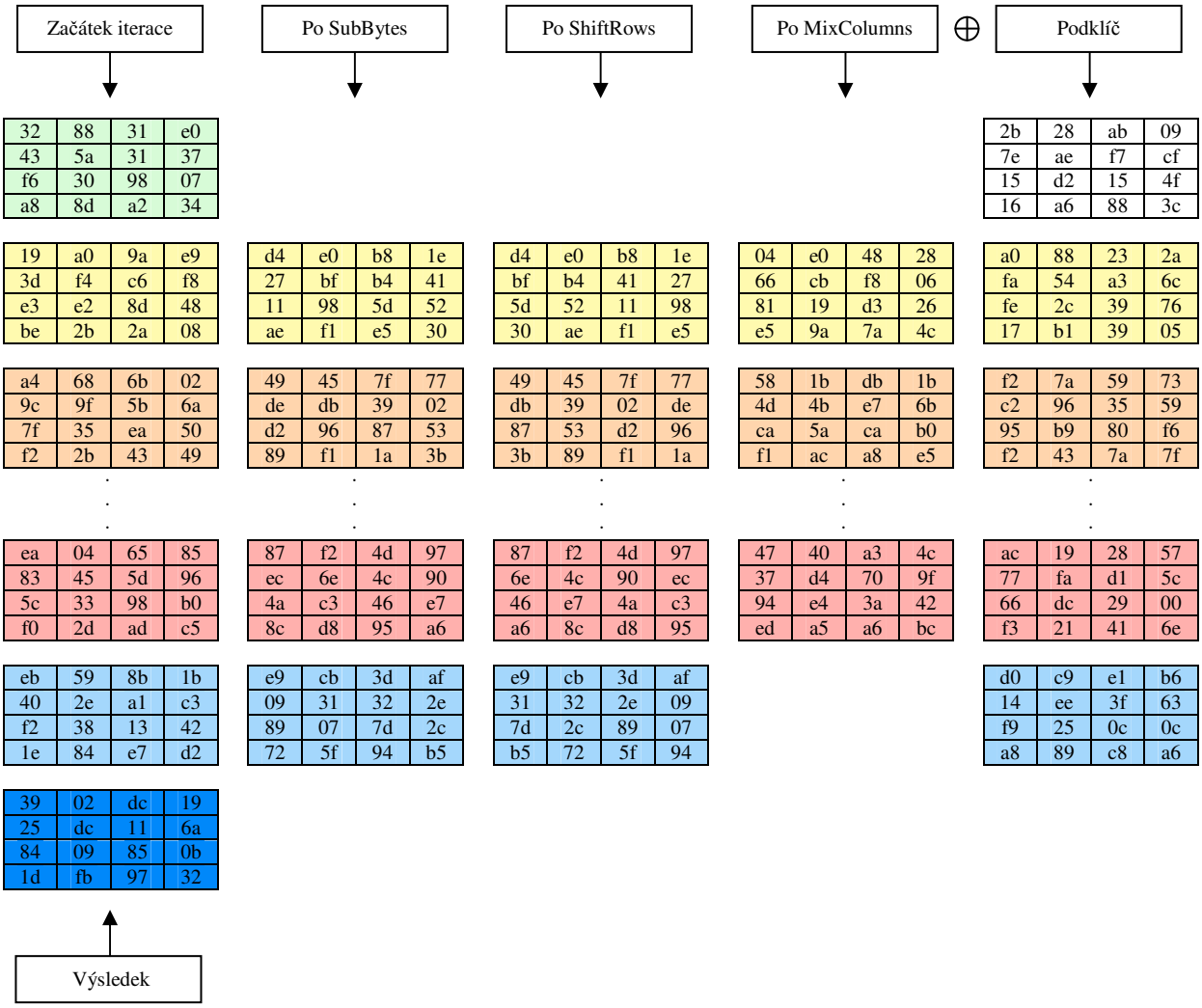
- **InvShiftRows** je cyklický posun řádků pole doprava a první řádek se neposouvá stejně jako u ShiftRows. Ostatní sloupce pak o jeden, dva a tři bajty doprava.

- **InvMixColumns** je transformace sloupců pole s využitím inverzní matice.

Na obrázku 4.8 je znázorněn zkrácený příklad šifrování metodou AES. Zeleně je ukázáno 16-ti bajtové pole vstupních nešifrovaných dat. Dále je přičten podklíč a následuje první iterace znázorněná žlutě. Oranžovou barvou je naznačena druhá iterace, červenou pak devátá a bleděmodře desátá iterace. Tmavomodrou barvou je označeno výsledné pole šifrovaných dat.

Sloupce na obrázku 4.8 reprezentují výsledky po jednotlivých operacích popsaných v předchozím textu.

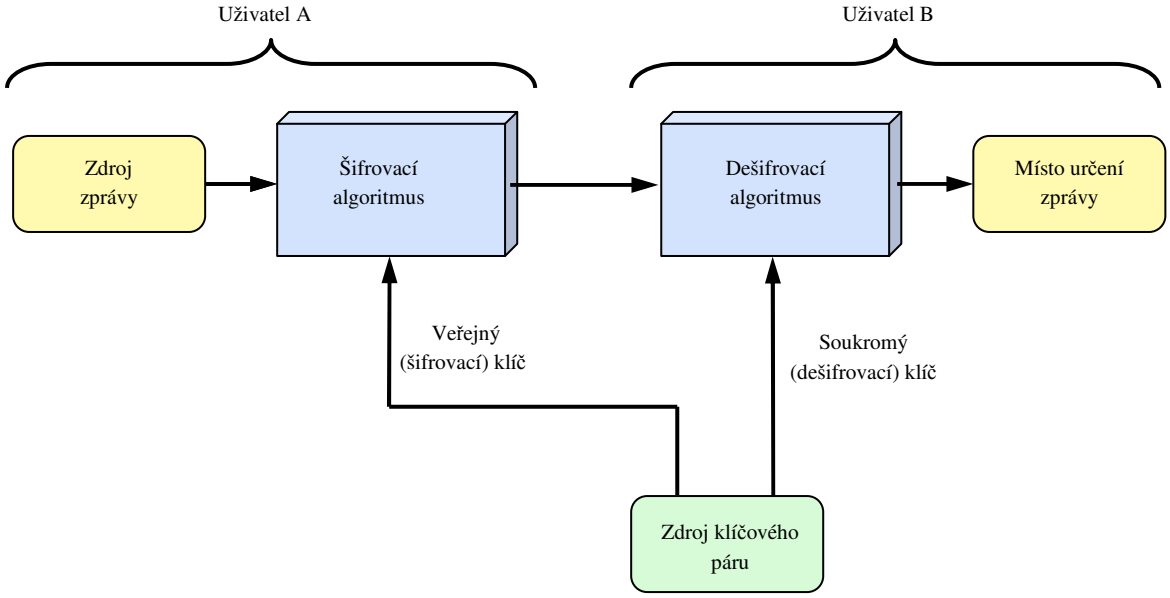
- Vstupní data: 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
- Šifrovací klíč: 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
- Výstupní šifrovaná data: 39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32



Obrázek 4.8 Zkrácený příklad šifrování metodou AES

4.2 Asymetrické kryptografie

U asymetrických šifrovacích metod, také nazývaných jako kryptografie s veřejným klíčem, je pro šifrování a dešifrování použito různých klíčů. Ty se pak označují jako veřejný a soukromý klíč, na rozdíl od symetrických šifrovacích metod, jež používají k šifrování i dešifrování jediný, tajný klíč. Toto je základní výhodou asymetrického šifrování, jelikož je eliminována výměna klíčů a kdokoli pomocí veřejného klíče zašifruje zprávu a pouze příjemce vlastnící soukromý klíč ji může dešifrovat. Utajení komunikace je pak jedním, ne však jediným využitím asymetrické kryptografie. Další aplikací je například elektronický podpis, umožňující prokázat u dat jejich autora [22].



Obrázek 4.9 Princip asymetrické kryptografie

Obvyklý způsob asymetrického šifrování je takový, že veřejný (šifrovací) klíč je volně zpřístupněn majitelem a kdokoli tímto klíčem může šifrovat jemu určené zprávy. Soukromý (dešifrovací) klíč majitel udržuje v tajnosti a pomocí něj tyto zprávy dešifruje. Na obrázku 4.9 je znázorněn princip šifrování veřejným klíčem. Je zřejmé, že uživatel A může mít k dispozici veřejné klíče od různých uživatelů nevyjímaje veřejného klíče od B. Pomocí něj zašifruje zprávu pro uživatele B. Jak již bylo napsáno, pouze uživatel B tuto zprávu dešifruje pomocí svého soukromého klíče B [25].

Obrácením principu na obrázku 4.9 je získán algoritmus digitálních podpisů, což je obdoba ručně psaných podpisů. Digitální podpisy zabezpečují autentičnost a integritu nebo autorství dokumentů. Berou v úvahu nejen informace o identitě podpisujícího, ale také informace v dokumentu obsažené. Tím je zaručeno že digitální podpis nelze připojit k libovolnému dokumentu. [26].

Z předchozího textu vyplývá, že šifrovací a dešifrovací klíč jsou matematicky svázány. Využívá se například jednocestných funkcí, které umožňující snadný výpočet výstupních dat ze vstupních, avšak opačně z výstupních dat nelze jednoduše určit data vstupní [23].

5 Bezpečnost bezdrátové komunikace

Bezdrátová komunikace poskytuje uživatelům v závislosti na technikách přenosu a použité technologii přístup k datům v definovaném akčním prostředí. Zejména rádiové sítě lze však velmi snadno odposlouchávat. Je to dáno tím, že se rádiový signál šíří i mimo prostory určené k přenosu dat. Tato rizika sebou přináší prakticky každá vybudovaná bezdrátová síť a nelze je technicky naprosto eliminovat. S pomocí směrových antén pak lze i z relativně velké vzdálenosti odposlouchávat provoz v síti, i když vysílače v této síti nemají výkonné antény. Další problémy přináší použité zabezpečovací metody, jelikož starší zařízení nemusí podporovat nejmodernější bezpečnostní systémy a celá síť je pak bezpečnostně omezena. Pak záleží na provozovateli, zda zvolí některé z nadstavbových metod zabezpečení na vyšší vrstvě, či nikoli. V dalším textu bude věnována pozornost zabezpečení přenosových technologií GPRS, Bluetooth a WiFi.

5.1 Zabezpečení GPRS

K jednoznačné identifikaci účastníka má každý mobilní uživatel přidělený jedinečný identifikátor IMSI, který se skládá z trojmístného kódu země MCC, dvoumístného kódu mobilní sítě MNC a desetimístného identifikačního čísla uživatele. IMSI je uloženo v SIM mobilního zařízení. Informace o zákazníkovi je uložena v mobilní síti domácího provozovatele v registru HLR [22].

5.1.1 Autentizace

Při každém přístupu k síti GSM/GPRS se musí uživatel autentizovat. Před tím než je navázána jakákoli relace, je nutná registrace. Během ní mobilní stanice vznáší požadavek na přístup do sítě a na základě toho je stanice autentizována.

Toto je tedy založeno na mechanizmu výzva-odpověď. Při autentizaci je v síti vygenerována náhodná 128 bitová hodnota. Na straně uživatele se autentizace provádí na SIM kartě, mechanizmem A3/A8. Na SIM pracují algoritmy specifické pro provozovatele, které jako vstup použijí náhodné číslo a privátní klíč uložený na SIM a vytvoří 32 bitovou odpověď a také 64 bitový klíč, následně užitý pro šifrování provozu. Přijatou odpověď si síť následně prověří proti vlastnímu výpočtu a na základě shody autentizuje uživatele. Privátní klíč uživatele se nikdy nepřenáší sítí.

Anonymita uživatelů je v sítích GSM/GPRS chráněná tím, že místo identifikátoru IMSI se používá dočasná identita TMSI a ta se používá při autentizaci. IMSI v otevřené podobě musí mobilní stanice poslat pouze jednou, při prvním kontaktu se sítí nebo pokud IMSI nelze získat jinak ve vazbě s aktuální TMSI [22].

5.1.2 Šifrování

Přenášená data jsou v síti GSM/GPRS chráněná při přenosu páteřní sítí a rádiovou částí sítě proti odposlechu pomocí šifrování. Podpůrný uzel GPRS a mobilní stanice používají 128 bitové náhodné číslo použité při autentizaci a privátní klíč uložený v SIM a také HLR. Prostřednictvím algoritmu A8 se vygeneruje šifrovací klíč. Data přenášená mezi uživatelem a sítí GPRS se šifrují pomocí algoritmu GPRS-A5, což je modifikovaná verze algoritmu A5 používaného pro šifrování hlasové komunikace v sítích GSM. Délka klíče (64 bitů) není již dostatečně silná pro potřeby současného zabezpečení komunikace [22].

5.2 Zabezpečení Bluetooth

Bluetooth poskytuje tři základní bezpečnostní služby. Autentizaci, což je ověření totožnosti komunikujících stran, důvěrnost, čili ochranu před odposloucháváním a autorizaci neboli povolení přístupu ke službám.

Specifikace nabízí tři bezpečnostní režimy:

- **Bez zabezpečení** – promiskuitní režim umožňující jakémukoli jinému zařízení navázat komunikaci.
- **Bezpečnost na úrovni služeb** – zajišťuje autorizaci přístupu ke službám na úrovni služeb.
- **Bezpečnost na úrovni spoje** – zařízení iniciuje bezpečnostní postupy, jako autentizaci a šifrování před vlastním spojením.

5.2.1 Inicializace

Řízení přístupu je možno zajistit volbou bezpečnostního režimu pro službu a úrovně důvěry vůči zařízení. Systémy Bluetooth se mohou vzájemně lokalizovat, nicméně komunikace může probíhat až po zásahu uživatele ve fázi inicializace. V této fázi se vzájemně komunikující stanice párují. Nejdříve se vygeneruje inicializační klíč na základě identického PIN na obou zařízeních, unikátní adresy vyzyvatele a čísla náhodně vygenerovaného ověřovatelem, které je odlišné pro každou transakci. Inicializační fáze je nejnebezpečnější, jelikož není nijak chráněna. Není doporučeno realizovat proces párování v místech, kde hrozí odposlech.

PIN je dlouhý 8 až 128 bitů a uživatel jej může zadávat ručně nebo může být uložen v paměti zařízení. Obvykle pouze zařízení s minimální pamětí a minimálním uživatelským rozhraním mají PIN pevně zadaný již ve výrobě.

Adresa v délce 48 bitů je jedinečná pro každé zařízení a je veřejná, stejně jako náhodné číslo v délce 128 bitů. To je však nepředvídatelné pro každou transakci.

5.2.2 Autentizace

Pro autentizaci zařízení se používá klíč spoje generovaný s pomocí inicializačního klíče. Tím může být buď klíč zařízení, kombinační klíč nebo hlavní klíč. Vlastní proces autentizace probíhající na úrovni spoje používá principu výzva-odpověď. Vyzyvatel zašle svoji adresu a od druhé komunikující strany dostane náhodné číslo. Na základě těchto hodnot a sdíleného klíče spoje se pomocí autentizační funkce spočítá výsledek, který si obě strany porovnají. Cílem je ověření znalosti sdíleného klíče druhou stranou.

Klíč zařízení se generuje při instalaci zařízení a aplikace při inicializaci rozhodne, čí klíč použije jako klíč daného spoje.

Kombinační klíč se po dohodě generuje ve fázi inicializace kombinací klíčů komunikujícího páru stanic. Je bezpečnější než použití klíče zařízením, který je stejný pro jakoukoli komunikaci daného zařízení.

Klíč spoje může být buď trvalý, nebo dočasný. Trvalý klíč lze použít ve stejném tvaru i pro další spojení, ale uživatel jej může změnit. Dočasný klíč slouží pouze pro danou relaci, kde všichni účastníci musí sdílet jeden hlavní klíč, který nahrazuje jednotlivé klíče spoje [22].

5.2.3 Šifrování

Šifrovací klíč se odvozuje od autentizačního klíče, ovšem pro každý paket nově. Délka šifrovacího klíče (8 až 128 bitů) se musí mezi komunikačními stranami předem dohodnout. Oddělení klíčů pak dovoluje použít slabší zabezpečení kratším klíčem, aniž by se ovlivnila síla autentizace. Vlastní režim šifrování pak závisí mj. na typu klíčového spoje. Pro autentizaci a generování klíčů se používají algoritmy vytvořené na bázi symetrického blokového algoritmu SAFER+ a pro šifrování symetrický proudový algoritmus na bázi posuvného registru s lineární zpětnou vazbou [22].

5.3 Zabezpečení WiFi

WiFi sítě nemají žádnou implicitně zabudovanou bezpečnost, nicméně nabízejí zabezpečení jako nedílnou volitelnou možnost. Od začátků implementace WLAN se pracuje na jejich lepším zabezpečení a nyní jsou k dispozici mechanismy, které dokážou zabezpečit WLAN i pro použití v nejpřísnějších podmínkách. Mimo to je nutné vzít v úvahu zabezpečení pomocí vymezení prostoru sítě a omezení průniku signálů. Čili vytvořit síť tak, aby pokrývala jen vymezený prostor. K tomu poslouží použití směrových antén, stavebních materiálů s minimalizací průniku signálu a další [8].

5.3.1 Obvyklé metody zabezpečení

Pro soupis základních metod zabezpečení bylo vycházeno z [4], [22].

- **Zablokování vysílání SSID.** Zablokováním vysílání SSID je sice porušen standard, nicméně pokud je síť zdánlivě skryta, jsou do jisté míry omezeny útoky na ni. Nepřijímání broadcastů s SSID je důvodem nezobrazení se seznamu dostupných bezdrátových sítí klientem. Avšak při připojování klienta k přípojnému bodu je SSID přenášen v otevřené podobě a lze ho tak snadno zachytit. Útočník může do bezdrátové sítě vysílat rámce, kterými vynucuje reasociaci přihlášených klientů. Pak již stačí zachytávat SSID a následně použít.

- **Kontrola MAC adres.** Access point bezdrátové sítě má k dispozici seznam MAC adres klientů, kterým je dovoleno se připojit. Pokud se chce útočník připojit do takovéto sítě s filtrováním MAC adres, musí se vydávat za stanici, která již byla v síti připojena. Toho docílí nastavením stejné MAC adresy na svém přístroji.

- **WEP** využívá symetrického šifrování pomocí statických WEP klíčů. Tyto jsou ručně nastaveny v obou komunikujících zařízeních. Nedostatky v protokolu umožňují prolomení zachycením specifických rámců. Klíč je získán následnou analýzou těchto rámců.

- **802.1X** je metoda odstraňující nedostatky zabezpečení WEP klíči. Access point je v této situaci autentizátorem, který řídí přístup do sítě. Uživatel nebo klient využívá na své straně program zvaný suplikant. AP zprostředkuje komunikaci s ověřovacím serverem (například RADIUS server), který vyžaduje autentizaci pomocí protokolu IEEE 802.1X. Po ověření má uživatel povolen přístup do sítě. Tato metoda je vhodná po bezdrátové přístupové body, jelikož mají obvykle malou paměť a malý výpočetní výkon.

- **WPA** využívá WEP klíče pro zajištění zpětné kompatibility, nicméně tyto jsou dynamicky měněny. Suplikant, což je doprovodný program, tuto změnu zajišťuje a proto je umožněno WPA implementovat i do starších zařízení. PSK nebo RADIUS server autentizuje přístup do WPA sítě.

- **WPA2** přináší uživatelům kvalitnější šifrování, avšak u některých výpočetních systémů je nutná jeho doinstalace. Vzhledem k vyšší výpočetní výkonnosti a šifrování AES, nelze WPA2 používat na starších zařízeních. Certifikace WPA2 je rozdělena do dvou kategorií a to pro podniky a pro osobní použití. V prvním případě jde o plnou podporu WPA2, včetně 802.1X a PSK. V druhém případě jsou požadavky na zabezpečení menší, tak postačuje pouze PSK.

6 Laboratorní pracoviště

V této kapitole je věnována pozornost laboratornímu pracovišti pro experimentální ověření jednotlivých přenosových metod. Nejprve budou vytvořeny přenosové modely jednotlivých bezdrátových technologií, dále rozebrány základní požadavky na mobilní systém a centrální počítač sběru dat. Následuje návrh mobilního systému s popisem jednotlivých hardwarových bloků a jejich realizace.

6.1 Přenosové modely

Jednotlivé přenosové modely vycházejí z informací obsažených v úvodu do použitých bezdrátových technologií v kapitole 1. Pro mobilní zařízení, pohybující se v okruhu větším než 1km je výhodné použít ke komunikaci GSM/GPRS viz obrázek 1.1. Zde již není obvykle ekonomicky výhodné vytvářet specializovanou síť. Krom prakticky neomezené dostupnosti nabízí GSM/GPRS v závislosti na počtu obsazených timeslotů přenosovou rychlost až 174 $kbit \cdot s^{-1}$.

Naproti tomu například ve výrobních prostorách a halách, kde dochází k migraci výrobních zařízení, případně jiných technologických celků, bývá rozumné vybudovat malou síť a jednotlivé zařízení k ní bezdrátově připojit a umožnit tak centralizovaný dohled a usnadnit tím také sběr dat. Zde se nabízí použití sítí WiFi nebo Bluetooth v závislosti na rozlehlosti pracovního prostoru a nabízeným službám. U těchto technologií bude v převážné většině případů využito Ad-hoc (Point to Point) a Infrastrukturních sítí. Ty je možné vidět na obrázku 1.3 a 1.4.

6.2 Rozbor požadavků

Při tvorbě laboratorního pracoviště je potřeba vzít v úvahu požadavky na něj kladené. Je tedy nutné vyřešit mobilní systém tak, aby modifikace na jednotlivé bezdrátové technologie probíhala jednoduše a efektivně a přitom byla zachována hardwarová struktura. Dále je potřeba rozhodnout, jak bude připojen centrální počítač pro sběr dat, nebo pro řízení mobilního systému.

Základní požadavky na mobilní systém jsou:

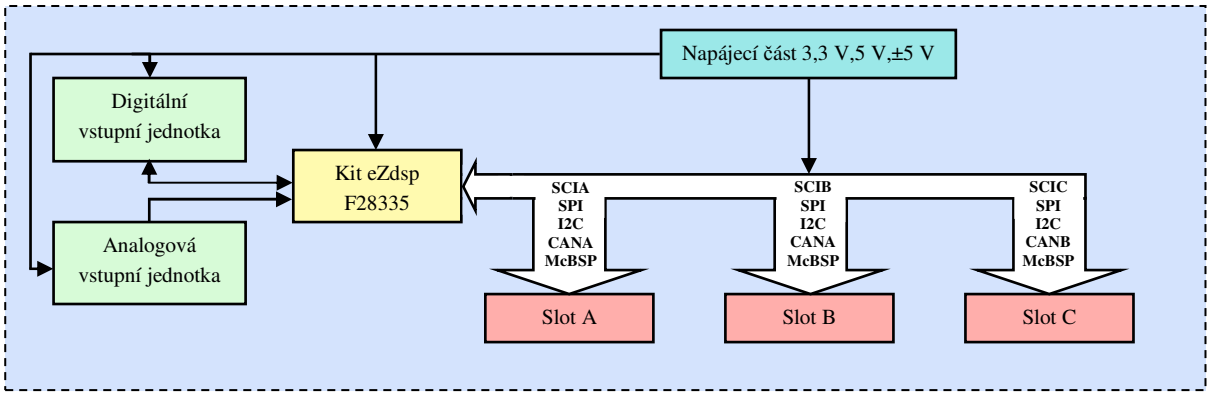
- Využití vývojového kitu eZdsp TMS320F28335.
- Možnost připojení externích analogových signálů.
- Přístup ke sběrnicím, které vývojový kit nabízí.
- Jednoduchá změna bezdrátové technologie.
- Možnost rekonfigurace na jinou strukturu sítě.
- Snadná rozšiřitelnost o další funkce.

Požadavky na centrální počítač řízení a sběru dat:

- Napojení počítače do sítě Internet.
- Integrace technologie Bluetooth, WiFi, GPRS a GPS.
- Software pro komunikaci s mobilním zařízením.

6.3 Návrh mobilního systému

Jak již bylo v předchozí kapitole naznačeno, je potřeba přistoupit k návrhu mobilního systému komplexně. Základní myšlenkou je vytvoření podpůrné desky pro kit eZdsp TMS230F28335. Ta musí obsahovat veškerý napájecí management, dále analogové a digitální galvanicky oddělené vstupy. Nezbytné je vyvedení komunikačních sběrnicí na rozšiřující sloty, do nichž budou připojeny nadstavbové moduly. Na obrázku 6.1 je znázorněna zjednodušená bloková struktura mobilního systému.



Obrázek 6.1 Bloková struktura mobilního systému

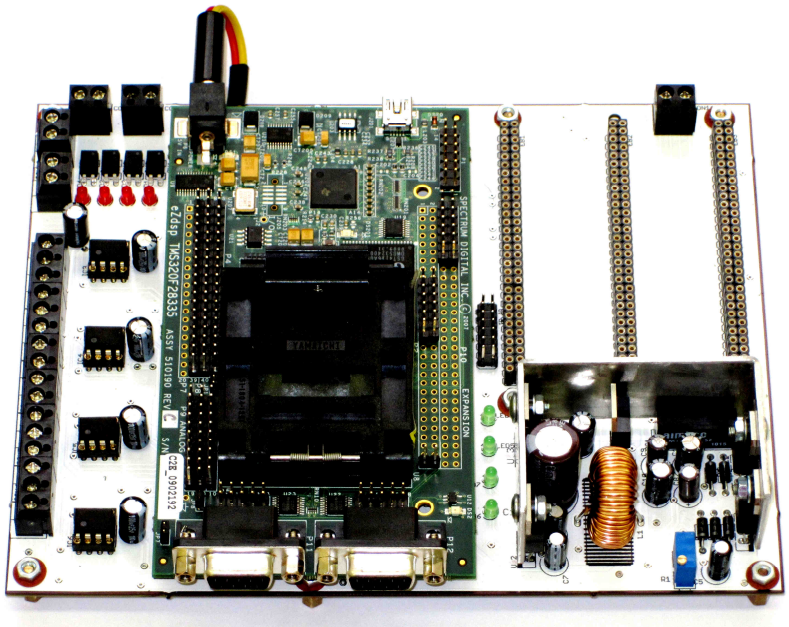
Napájecí část je řešena několika zdroji napětí. Spínaným stabilizovaným zdrojem 5 V a lineárním stabilizovaným zdrojem 3,3 V pro napájení číslicové části, dále stabilizovaným zdrojem ±5 V analogové vstupní jednotky. Je tedy k dispozici několik úrovní napájecího napětí (3,3 V, 5 V, ±5 V). Tím je zajištěna kompatibilita s různými nadstavbovými moduly. Napájecí napětí je rozvedeno po celé podpůrné desce, jsou jím napájeny veškeré obvodové struktury a je i vyvedeno na jednotlivých slotech.

Kit eZdsp TMS320F28335 se signálovým procesorem koordinuje veškeré datové toky mezi sloty, potažmo nadstavbovými moduly. Dále převádí analogová napětí z analogové vstupní jednotky pomocí integrovaného AD převodníku na digitální data, se kterými je dále pracováno. Digitální vstupní jednotka je také připojena prostřednictvím kitu k signálovému procesoru.

Analogová vstupní jednotka obsahuje osm vstupů a upravuje vstupní signály na bezpečné hodnoty pro AD převodník obsažený v procesoru na kitu. Vzhledem k omezenému vstupnímu rozsahu AD převodníku (0-3 V) byl navržen obvod, upravující vstupní rozsah napětí ±15 V na hodnoty 0-3 V. Byl kladen důraz na nízké zvlnění napětí na vstupech AD převodníku, které je menší než 1 mV.

Digitální vstupní jednotka galvanicky odděluje čtyři vstupní číslicové signály vhodné například pro řízení a signalizaci. Hlavním úkolem této části je chránit GPIO piny před případným zničením. Vstupní úroveň je signalizována LED.

Sloty, jak naznačuje obrázek 6.1, umožňují připojení široké škály nadstavbových modulů pomocí jednotlivých rozhraní (SCI, SPI, I2C, McBSP, CAN). Jsou zde také vyvedeny PWM výstupy z kitu a některé GPIO signály pro případné pozdější využití.



Obrázek 6.2 Podpůrná deska s osazeným kitem eZdsp TMS320F28335

6.4 Hardwarové moduly

Pro tvorbu mobilního systému jsou využity komerčně dostupné moduly. Pro jednotlivé bezdrátové technologie byly vytvořeny rozšiřující desky podobné koncepce, zajišťující modularitu mobilního systému. Mimo rozšiřujících desek je také použit řídicí systém se signálovým procesorem, GPS přijímač a trakční elektroměr.

6.4.1 Kit eZdsp F28335

Je kompletní vývojová platforma pro sérii procesorů TMS320F28xxx s plovoucí řádovou čárkou. Tento kit je koncipován na procesoru TMS320F28335 (obrázek 6.3). Obsahuje integrovaný JTAG emulátor, 128k x 16 synchronní SRAM, precizní patici pro procesor, CAN rozhraní (v provedení konektoru Canon 9 a 9 pinový DSUB) a RS-232 rozhraní ve stejném provedení. Dále pak rozšířenou sběrnici poskytující přístup ke všem I/O signálům mikroprocesoru. Pro vyhodnocení stavů procesoru je na kitu osazena LED, kterou je možno ovládat přes GPIOF. Na jumperovém poli je možné nastavit BOOT mode (paralelní port, flash, SPI, SCI, vnitřní paměť). Samozřejmostí je také uživatelské USB rozhraní pro komunikaci s nadřazeným osobním počítačem. Komplet také obsahuje napájecí zdroj a vývojový software Code Composer Studio™ v3.3 [30].

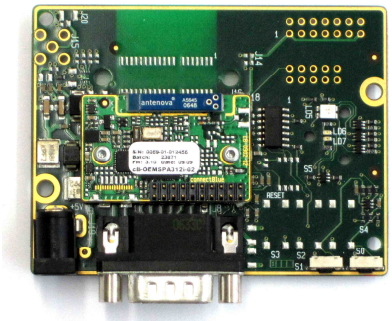
Signálový procesor s plovoucí řádovou čárkou TMS320F28335 použitý v mikropočítačovém systému má jádro taktováno pomocí PLL až do 150 MHz, čímž jeden cyklus a jedna instrukce pak díky využití PIPELINE trvá právě 6,67 ns. Jádro je napájeno napětím o hodnotě 1,9 V a veškeré I/O piny pracují s napěťovou hladinou 3,3 V, kromě ADC jež má přípustné maximálně 3 V. Procesor využívá Harvardskou architekturu s šířkou slova 32 bitů. Má implementovanou hardwarovou násobičku s 32 bit x 32 bit násobením případně duální 16 bit x 16 bit. Čip obsahuje také 256 k x 16 bit FLASH, 34 k x 16 bit paměti SRAM a také Boot ROM 8 k x 16 se softwarovými boot módy a standardními matematickými tabulkami [30].

Obrázek 6.3 Kit eZdsp TMS320F28335

Pro komunikaci s okolím je k dispozici široká škála rozhraní (2 x CAN2.0, 3 x SCI, 2 x McBSP, 1 x SPI, 1 x I2C). Samozřejmostí je 18 PWM výstupů, 6 HRPWM výstupů, 6 Event Capture vstupů, osm 32 bit nebo šest 16 bit čítačů/časovačů, 2 x QEP jednotky pro vyhodnocení signálů z inkrementálního čidla, 2 osmi-kanálové 12 bit ADC se sample and hold jednotkou. Procesor disponuje 88 programovatelnými I/O piny se vstupní filtrací [30].

6.4.2 OEM RS232 Module Adapter III

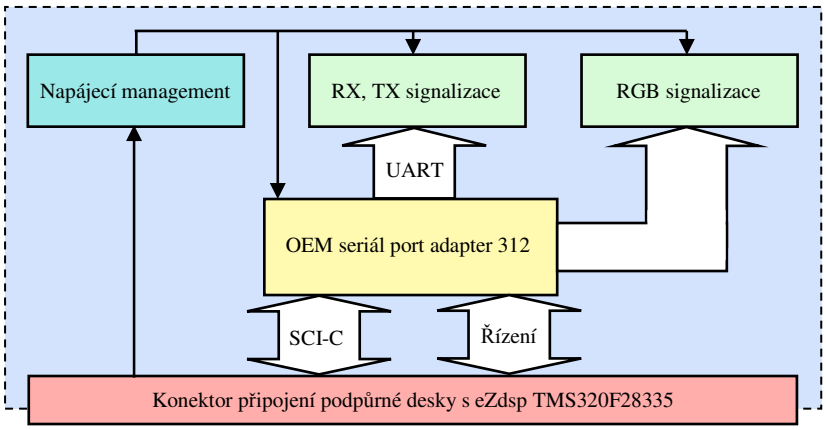
Tento adaptér umožní Bluetooth konektivitu personálního počítače prostřednictvím RS232 komunikačního rozhraní. Na obrázku 6.4 je znázorněn s připojeným modulem OEM serial port adapter™ 312, jehož bližší popis je uveden v kapitole 5.4.3. Díky tomuto adaptéru je umožněn vývoj Bluetooth aplikací na personálním počítači, komunikace s Bluetooth moduly a jejich nastavení pomocí programu SPA Toolbox, nebo AT+i příkazy. Moduly se připojují přes šedesáti pinový dvouřadý konektor obsažený na adaptéru. Dále jsou k dispozici LED indikující přenos dat, a RGB LED informující o stavu modulu. Adaptér také obsahuje tlačítko pro uvedení modulu do základního nastavení, a univerzální funkční tlačítko. Napájení adaptéru je řešeno 5V adaptérem nebo kabelem připojeným do USB portu personálního počítače [31].



Obrázek 6.4 OEM RS232 Module Adapter III

6.4.3 Bluetooth rozšiřující deska

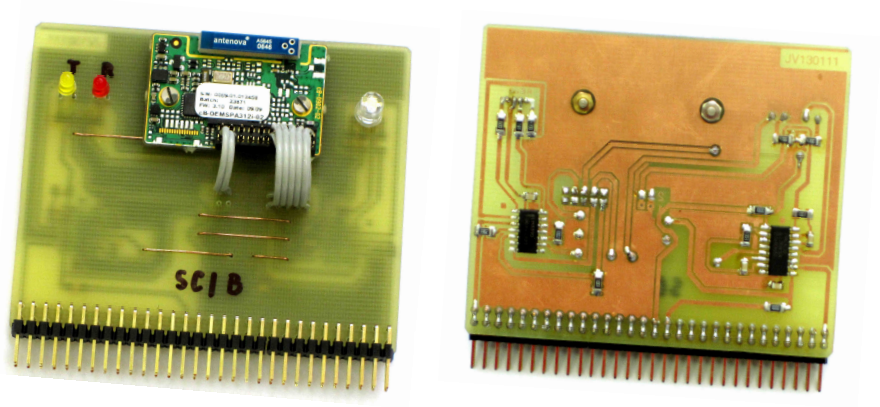
Komunikace mobilního systému s personálním počítačem, nebo jiným zařízením prostřednictvím Bluetooth, je zajištěna Bluetooth rozšiřující deskou. Na zjednodušeném blokovém schématu (obrázek 6.5) je znázorněno propojení mezi jednotlivými pomocnými obvody, modulem OEM serial port adapter™ 312 a šedesáti pinovým dvouřadým konektorem, jež slouží k propojení s podpůrnou deskou. Deska obsahuje signalizační obvody stavu sběrnice a budič RGB LED informující o stavu modulu. Celkovou sestavu znázorňuje obrázek 6.6.



Obrázek 6.5 Blokové schéma Bluetooth rozšiřující desky

OEM serial port adapter™ 312 je Bluetooth modul založený na bázi systému Philips BGB203. Systém BGB203 má na čipu SRAM a FLASH ve stejném pouzdru. K dispozici je

sériové rozhraní RS232 nebo UART, které podporuje i nestandardní modulační rychlosti. Modul má integrovanou anténu s vysílacím výkonem 49 mW. Napájecí napětí modulu je 3 - 6 V a napěťové úrovně na I/O pinech jsou 3,3 V. Třída rádia 1 předurčuje modul k využití přenosu až do 100 m. Podporuje Bluetooth klasifikaci 2.0. Jeho ovládání probíhá prostřednictvím AT+i příkazů [32].



Obrázek 6.6 Bluetooth rozšiřující deska

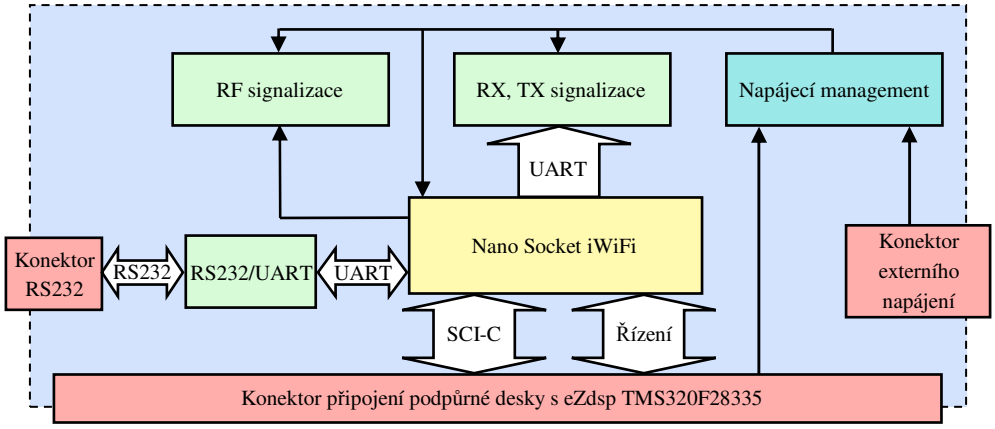
Jsou podporovány následující Bluetooth profily:

- Obecný přístupový profil (GAP)
- Serial port profil (SPP)
- Profil vytáčeného propojování (DUN GW, DUN DT)

6.4.4 WiFi rozšiřující deska

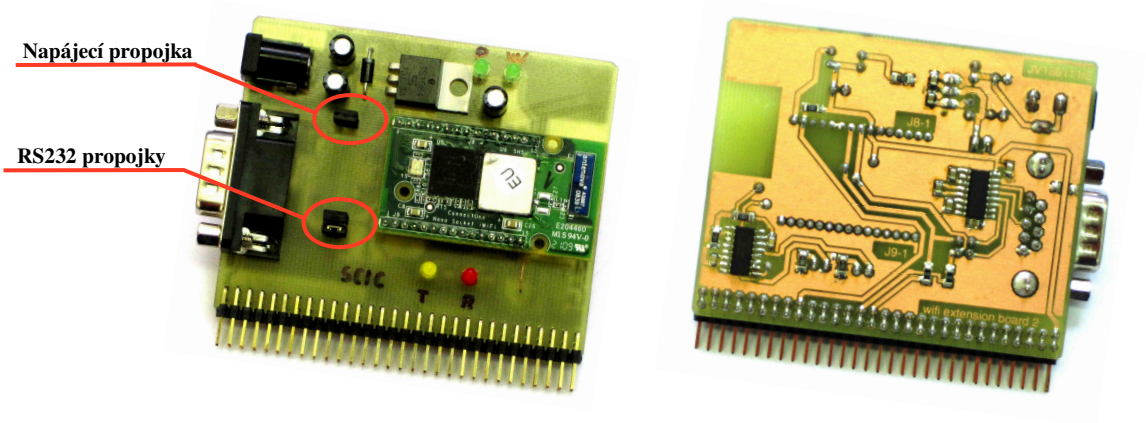
Pro připojení mobilního systému k WiFi byla vytvořená rozšiřující deska, jejíž zjednodušené blokové schéma je na obrázku 6.7. Přináší možnost komunikace se sériovou linkou personálního počítače prostřednictvím konektoru Canon 9. Takto lze jednoduše konfigurovat osazený modul Nano Socket iWiFi a také rozšiřující desku samostatně využít například pro tvorbu AP. Dále deska obsahuje nadstavbový napájecí management a šedesáti pinový dvouřadý konektor pro integraci do podpůrné desky s kitem eZdsp TMS320F28335. Součástí WiFi rozšiřující desky jsou také signalizační obvody zobrazující stav na komunikační sběrnici a aktivitu RF vysílače. Rozšiřující WiFi deska je znázorněna na obrázku 6.8.

Na WiFi rozšiřující desce jsou obsaženy tři jumperové propojky. Umožňují základní funkční konfiguraci, pro případ samostatného použití bez integrace do podpůrné desky. Propojením napájecí propojky je modul Nano Socket iWiFi napájen přímo z rozšiřující desky prostřednictvím integrovaného stabilizovaného zdroje napětí 3,3 V. Také je umožněna RS232 komunikace prostřednictvím konektoru Canon 9 v případě propojení RS232 propojek. Na obrázku 6.8 jsou propojky znázorněny a popsány.



Obrázek 6.7 Blokové schéma WiFI rozšiřující desky

Využití modulu s integrovaným software Nano Socket iWiFi™, nabízí velmi jednoduchou možnost, jak hostitelský systém připojit k WiFi konektivitě bez nutnosti instalace jakýchkoli ovladačů. Propojení s hostitelským systémem umožňuje široká škála dostupných rozhraní (UART, SPI, RMII). Modul odděluje aplikace s vysokým zabezpečením od sítě, podporuje deset paralelních TCP/UDP spojení a další. Také implementuje web server s dvěmi web stránkami (zákaznická a konfigurační). Podporuje SMTP a POP3 protokoly, příslušenství MIME, FTP a TELNET a SerialNET™ mód pro Serial-to-IP bridging. Modul je ovládán pomocí AT+i příkazů. Jádro pracuje s napětím 1,2 V zatímco I/O porty s 3,3 V. Díky nabídce několika energeticky úsporných režimů je možno optimalizovat spotřebu modulu dle aktuálních požadavků [33].



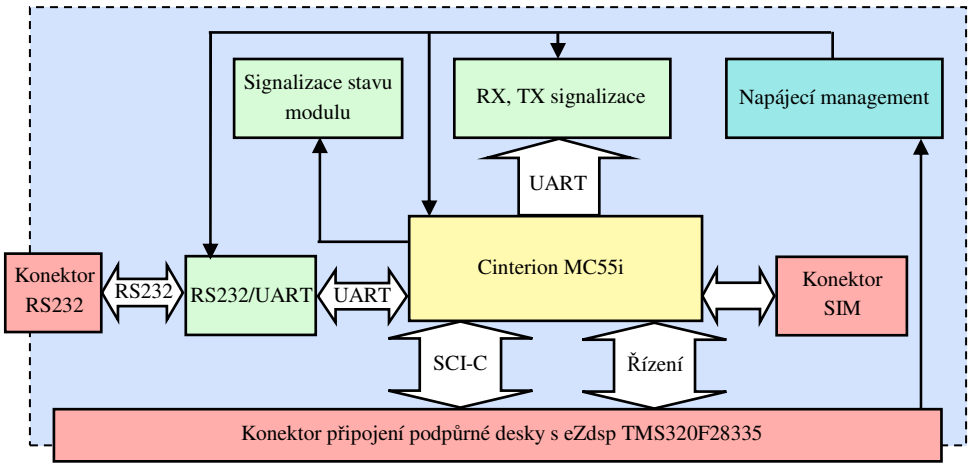
Obrázek 6.8 WiFi rozšiřující deska se znázorněním konfiguračních propojek

Podporované internetové protokoly:

- ARP, ICMP, IP, UDP, TCP, DHCP, DNS, NTP, SMTP, POP3, MIME, HTTP, FTP a TELNET.
- Zabezpečené protokoly: SSL3/TLS1, HTTPS, FTPS, RSA, AES-128/256, 3DES, RC4, SHA-1, MD-5, MD-2, WEP, WPA/WPA2 (PSK a Enterprise).
- Protokoly akcelerované v hardware: AES, 3DES a SHA.

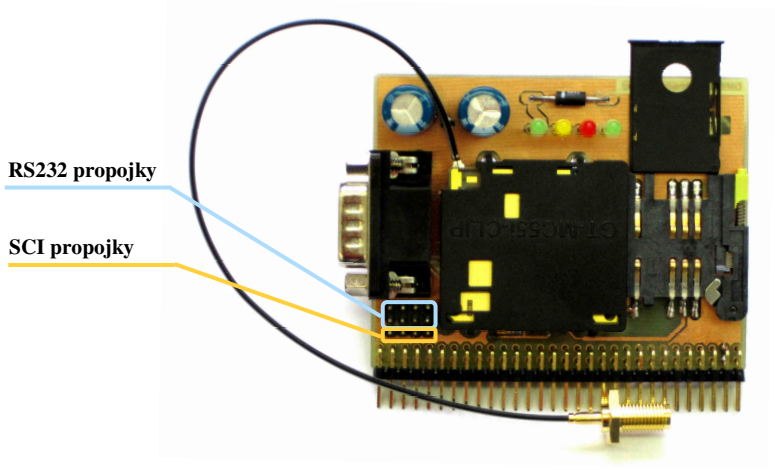
6.4.5 GSM/GPRS rozšiřující deska

Rozšiřující deska pro komunikaci prostřednictvím GSM/GPRS je vytvořena ve stejném hardwarovém formátu jakou předchozí desky s technologiemi Bluetooth a WiFi. Pro GSM/GPRS technologii je využit modul firmy Cinterion MC55i. Blokové schéma na obrázku 6.9 uvádí základní propojení mezi jednotlivými dílčími bloky. Napájecí management zabezpečuje úpravu napájecího napětí pro modul MC55i a zároveň zajišťuje malé zvlnění napájecího napětí při vysílání, kdy vznikají poměrně velké proudové špičky (1,9 A). Pro funkci modulu MC55i je nezbytně nutná externí čtečka SIM karet, která je implementována na GSM/GPRS rozšiřující desce. Samozřejmostí jsou signalizační obvody, informující o vysílaných a přijímaných datech na sběrnici a stavu modulu. Prostřednictvím konektoru Canon 9 je taktéž umožněna komunikace s RS232 linkou, volitelně s hardwarovým řízením toku. Proto je na rozšiřující desce integrován převodník RS232/UART.



Obrázek 6.9 Blokové schéma GPRS rozšiřující desky

Také GSM/GPRS rozšiřující deska obsahuje konfigurační propojky (obrázek 6.10). Propojením RS232 konfiguračních propojek je umožněna RS232 komunikace včetně hardwarového řízení toku prostřednictvím konektoru Canon 9 integrovaného na rozšiřující desce.



Obrázek 6.10 GSM/GPRS rozšiřující deska s naznačením konfiguračních propojek

Pomocí SCI propojek je provedeno spojení s konektorem podpůrné desky. Rozpojení propojek SCI umožňuje v případě integrace do rozšiřující desky s kitem eZdsp TMS320F28335 využít napájecího napětí, prostřednictvím konektoru připojení podpůrné desky a zároveň komunikaci přes propojenou RS232 linku konektorem Canon 9. Toto řešení je aktuální při ladění nastavení AT příkazy z personálního počítače.

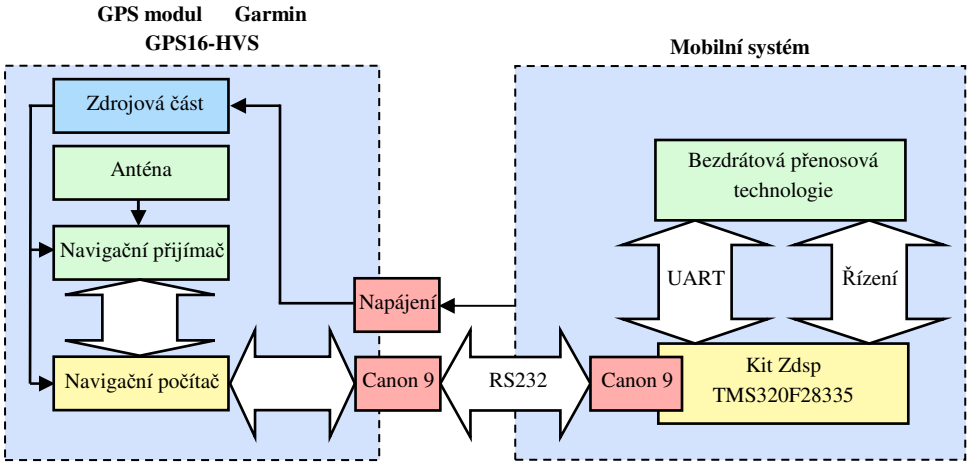
MC55i je čtyř pásmový (GSM/GPRS 850/900/1800/1900MHz) modul umožňující hlasové a datové služby založené na GPRS multi-slot třídy 10. Výstupní vysílací výkon pro GSM850 a GSM900 se pohybuje ve třídě 4, což odpovídá 2 W. Pro GSM1800 a GSM1900 se jedná o třídu 1, jejíž ekvivalentní výkon je 1 W. Modul je ovládán AT příkazy, které umožňují jeho využití bez nutnosti instalace ovladačů na hostitelském systému. Pomocí AT příkazů je taktéž umožněn přístup k TCP/IP. Na modulu je k dispozici anténní konektor pro připojení externí antény a padesáti pinový konektor obsahující piny napájení, rozhraní pro kartu SIM, audio vstupy/výstupy a dvě sériová rozhraní. Napájecí napětí modulu je 3,3–4,8 V [34].

Podporované internetové protokoly:

- IP, UDP, TCP, HTTP, FTP, SMTP, POP3

6.4.6 GPS modul

V určitých situacích je vyžadováno snímání polohy mobilního zařízení. To sebou přináší výhody v podobě přesného dohledu nad mobilním systémem. Přenášená data jsou pak doplněna informacemi o poloze, aktuálním čase, rychlosti pohybu, směru pohybu a nadmořské výšce. Na obrázku 6.11 je naznačeno propojení mobilního systému s GPS přijímačem firmy Garmin. Jedná se o typ GPS16-HVS (obrázek 6.12). Je patrné, že GPS přijímač je propojen prostřednictvím sériového rozhraní RS232 přímo s procesorovým kitem eZdsp 320F28335, jež má implementován převodník úrovní UART/RS232. konektor Canon 9 pak slouží k propojení kitu a GPS přijímače.

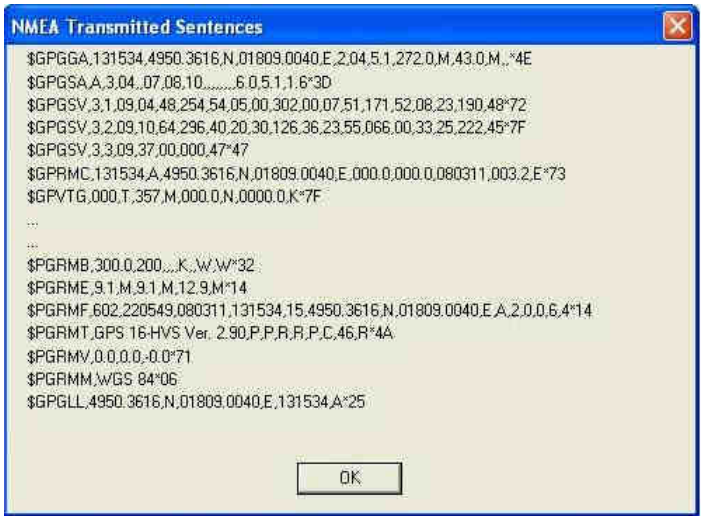


Obrázek 6.11 Propojení GPS přijímače a mobilního systému

Přijímač GPS16-HVS obsahuje interní anténu a je propojen RS232 komunikačním kanálem. Vypočítává polohu až z 12 satelitních vysílačů. Aktualizace dat polohy probíhá defaultně každou sekundu, avšak tento interval může být změněn. Přijímač podporuje DGPS, což je tzv. diferenciální GPS, využívající korekčních signálů přijímaných z jiných tzv. referenčních stanic, které se nacházejí ve známé poloze a pomocí nichž je možno definovat velikost chyby. Toto dovoluje zvýšit přesnost na 3 až 5 metrů. Díky integrované paměti FLASH, jsou zaznamenána veškerá nastavení a poslední poloha po vypnutí napájení. To usnadní počáteční konfiguraci a urychlí výpočet polohy po opětovném zapnutí napájení. Přijímač také umožňuje konfigurovat formát vysílaných dat na RS232. Je využíván datový protokol NMEA. Rozsah napájecího napětí je 8 – 40 V. Pro rychlou konfiguraci a kontrolu GPS přijímače pomocí personálního počítače je k dispozici konfigurační software. Umožňuje nejen měnit parametry komunikace, formát vysílaných dat a nastavení zpřesňujících algoritmů, ale také například přehrát novější firmware [35].

Obrázek 6.12 GPS modul

Na obrázku 6.13 je znázorněn příklad datového protokolu NMEA. Pro základní aplikace jsou podstatná data ze zpráv GPGGA, GPRMC, GPVGT, případně GPGSA. Význam jednotlivých segmentů ve zprávě je určen standardem NMEA.



Obrázek 6.13 Příklad datového protokolu NMEA

Pro objasnění jsou dále v tabulkách 6.1, 6.2, 6.3 uvedeny příklady a významy zpráv NMEA protokolu, konkrétně GPRMC, GPGGA a GPVGT. Zpráva začíná identifikátorem a jednotlivé segmenty ve zprávách jsou odděleny čárkou. Na konci zprávy je za znakem * uveden kontrolní součet, využívaný pro kontrolu správnosti příjmu zprávy.

$GPRMC,131534,A,4950.3616,N,01809.0040,E,000.0,000.0,080311,003.2,E*73

131534	UTC čas ve formátu hhmmss (hodina – minuta – sekunda)
A	Platnost zobrazovaných dat (A – platná pozice, V – neplatná pozice)
4950.3616	Zeměpisná šířka ve formátu ddmm.mmmm (stupně – minuty.desetinné vyjádření zbytku)
N	Určení polokoule u zeměpisné šířky (N – severní, S – jižní)
01809.0040	Zeměpisná délka ve formátu dddmm.mmmm (stupně – minuty.desetinné vyjádření zbytku)
E	Určení polokoule u zeměpisné délky (E – východní, W – západní)
000.0	Rychlost 000.0 až 999.9 uzlů
000.0	Azimut pohybu 000.0 až 359.9 stupňů
080311	UTC datum ve formátu ddmmrr (den – měsíc – rok)
003.2	Magnetická odchylka 000.0 až 180.0 stupňů
E	Směr magnetické odchylky (E – východ, W – západ)
*73	Kontrolní součet

Tabulka 6.1 Reprezentace jednotlivých znaků v GPRMC slově

$GPGGA,133856,4950.3616,N,01809.0040,E,2,04,5.1,272.0,M,43.0,M,,*4E

131534	UTC čas ve formátu hhmmss (hodina – minuta – sekunda)
4950.3616	Zeměpisná šířka ve formátu ddmm.mmmm (stupně – minuty.desetinné vyjádření zbytku)
N	Určení polokoule u zeměpisné šířky (N – severní, S – jižní)
01809.0040	Zeměpisná délka ve formátu dddmm.mmmm (stupně – minuty.desetinné vyjádření zbytku)
E	Určení polokoule u zeměpisné délky (E – východní, W – západní)
2	Indikátor GPS kvality (0=bez opravy, 1=oprava dostupná, 2=Diferenční GPS, 6=estimováno)
04	Počet dostupných satelitů, 00 až 12
5.1	Horizontální přesnost, 0.5 až 99.9
272.0	Nadmořská výška, -9999.9 až 99999.9 m
M	Identifikátor
43.0	Výška nad geoidem, -999.9 až 9999.9 m
M	Identifikátor
*4E	Kontrolní součet

Tabulka 6.2 Reprezentace jednotlivých znaků v GPGGA slově

$GPVTG,000,T,357,M,000.0,N,0000.0,K*7F

000	Správný směr vůči zemi, 000 až 359° (poprvé se pošlou nuly)
T	Identifikátor
357	Magnetický směr vůči zemi, 000 až 359°
M	Identifikátor
000.0	Rychlost v uzlech, 000.0 až 999.9 uzlů
N	Identifikátor
0000.0	Rychlost v kilometrech za hodinu, 0000.0 až 1851.8 $km \cdot h^{-1}$
K	Identifikátor
*7F	Kontrolní součet

Tabulka 6.3 Reprezentace jednotlivých znaků v GPVGT slově

6.4.7 Elektroměr EM4T

Při požadavcích na přesná měření elektrické energie trakčních vozidel lze využít hotového elektroměru (obrázek 6.14) vyvinutého pro tyto aplikace. Jedná se tedy o jednofázový trakční elektroměr umožňující jak jednosystémová, tak i dvousystémová měření. Konkrétní parametry elektroměru znázorňuje tabulka 6.4.

Obrázek 6.14 Elektroměr EM4T

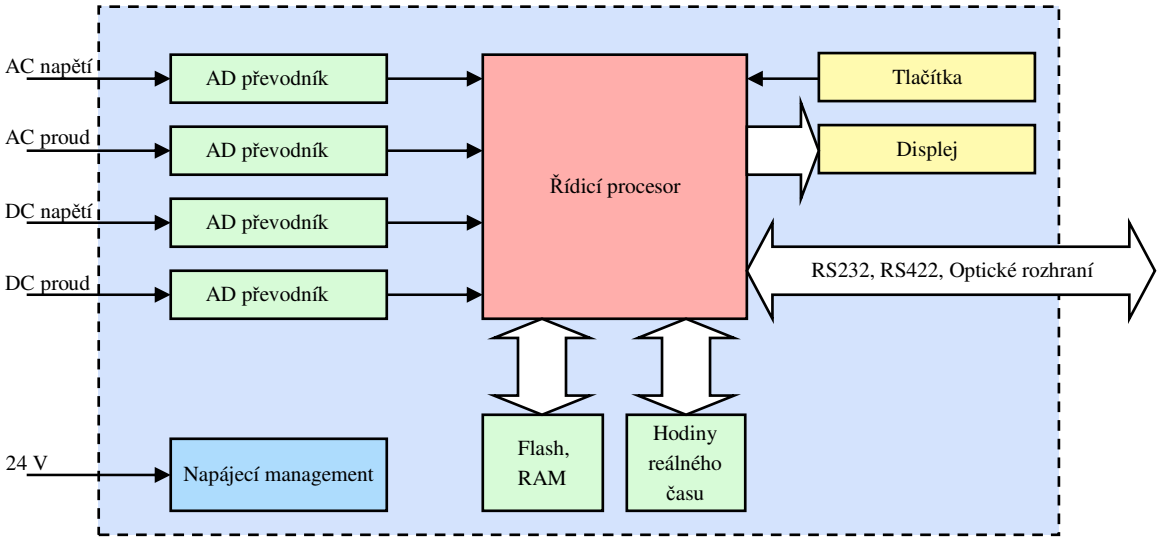
Ze základních parametrů vyplývá, že pro připojení ke konkrétnímu trakčnímu vozidlu bude nutné přizpůsobit vstupní veličiny použitím vhodných snímačů. U vícesystémových trakčních vozidel je výhodou dvousystémové provedení, umožňující současné připojení stejnosměrných i střídavých snímačů bez nutnosti jejich přepínání.

Měřicí rozsahy	Napětí	DC: 50 mA
		AC: 300 V
	Proud	DC: 0,1 A
		AC: 0,1 A
Frekvenční rozsah		DC, 50Hz
Rozlišení AD převodníku		16 bit
Vzorkovací frekvence		4000 Hz
Třída přesnosti		0,2
Komunikační sběrnice		RS232, RS422, optické rozhraní

Tabulka 6.4 Základní parametry elektroměru EM4T

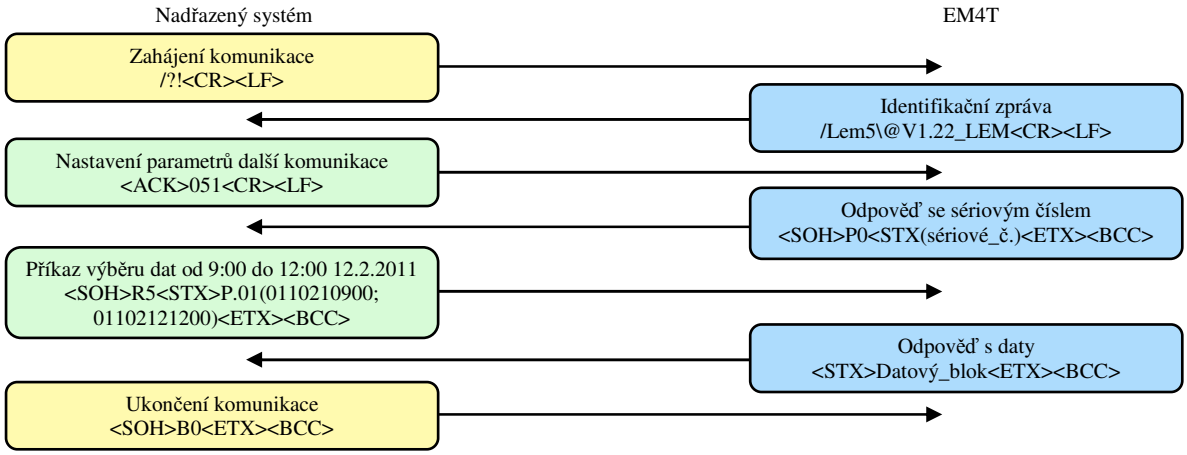
Na zjednodušeném blokovém schématu (obrázek 6.15) je znázorněn princip funkce dvousystémového provedení elektroměru EM4T. Vstupní střídavé a stejnosměrné signály, reprezentující změřená napětí a proudy, jsou přivedeny na jednotlivé rozdílové vstupy AD převodníků. Toto řešení umožňuje současně získávat hodnoty jednotlivých měřených veličin. Řídicí procesor dále tyto údaje zpracovává a zajišťuje požadované výpočty spotřeby respektive rekuperace elektrické energie. Dále procesor tyto data ukládá, včetně informací

z hodin reálného času a zvláštních událostí do flash paměti a prostřednictvím dostupných rozhraní komunikuje s nadřazeným systémem. Flash paměť má kapacitu na uchování záznamů o spotřebě elektrické energie za dobu cca 300 dnů, pokud je standardní interval záznamu 15 minut [36]. Elektroměr obsahuje také pomocná tlačítka a displej, který cyklicky informuje o aktuálních hodnotách spotřebované a rekuperované elektrické energie a připojené napájecí síti a podobně.



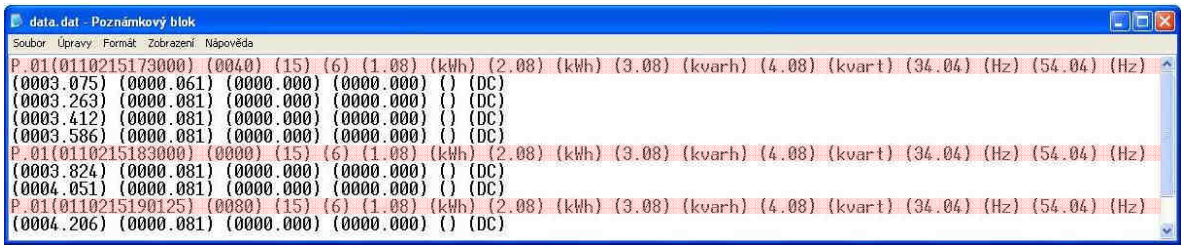
Obrázek 6.15 Zjednodušené blokové schéma elektroměru EM4T

Komunikace elektroměru s nadřazeným systémem probíhá prostřednictvím RS232, RS422 nebo optického rozhraní. Pokud nastane potřeba vyčíst data z paměti elektroměru, je nutné postupovat dle diagramu na obrázku 6.16. Používají se příkazy definované komunikačním protokolem elektroměru EM4T [36].



Obrázek 6.16 Příklad komunikace mezi EM4T a nadřazeným systémem při vyčítání dat

Příklad krátkého výpisu vyčtených dat z elektroměru EM4T je znázorněn na obrázku 6.17. Jedná se o ještě nezpracovaná data. Záznam je pokaždé uvozen hlavičkou (zvýrazněna červeně) a význam jednotlivých částí je popsán v dalším textu a tabulce 6.5.



Obrázek 6.17 Příklad výpisu nezpracovaných dat z elektroměru EM4T

Pro první hlavičku konkrétně:

P.01	EDIS kód
(0110215173000)	datum a čas uložení naměřených hodnot (rok, měsíc, den, hodina, minuta, sekunda)
(0040)	Stavové slovo
(15)	Perioda záznamu v minutách
(6)	Počet zaznamenaných proměnných
(1.08)	Kladná činná energie (činná energie spotřebovaná ze zdroje)
(kWh)	Jednotka
(2.08)	Záporná činná energie (činná energie rekuperovaná do zdroje)
(kWh)	Jednotka
(3.08)	Kladná jalová energie (induktivní jalová energie odebíraná ze zdroje)
(kvarh)	Jednotka
(4.08)	Záporná jalová energie (kapacitní jalová energie odebíraná ze zdroje)
(kvarh)	Jednotka
(34.04)	Typ napájecí sítě připojené na první dvojici vstupních kanálů elektroměru
(Hz)	Jednotka
(54.04)	Typ napájecí sítě připojené na druhou dvojici vstupních kanálů elektroměru
(Hz)	Jednotka

Tabulka 6.5 Význam jednotlivých částí hlavičky

Vypočítané hodnoty a typ napájecí sítě jsou vždy vypisovány na nový řádek ve stanovených intervalech konkrétně každých 15 minut. Jejich pořadí je stejné jako v hlavičce. Pokud nastane událost, kdy se změní hodnota stavového slova, je vytvořena nová hlavička. Tabulka 6.6 uvádí soupis stavových slov a v závislosti na událostech [36].

0000	Žádna událost
0001	Je nenulový funkční chybový registr
0002	Slabá baterie
0010	Vynulování 1.08, 2.08, 3.08, 4.08
0020	Byl nastaven čas, datum, nebo číslo vlaku
0040	Připojení napětí
0080	Odpojení napětí
00C0	Odpojení a připojení napětí
0100	Nastavení proměnných
2000	Vymazána paměť události

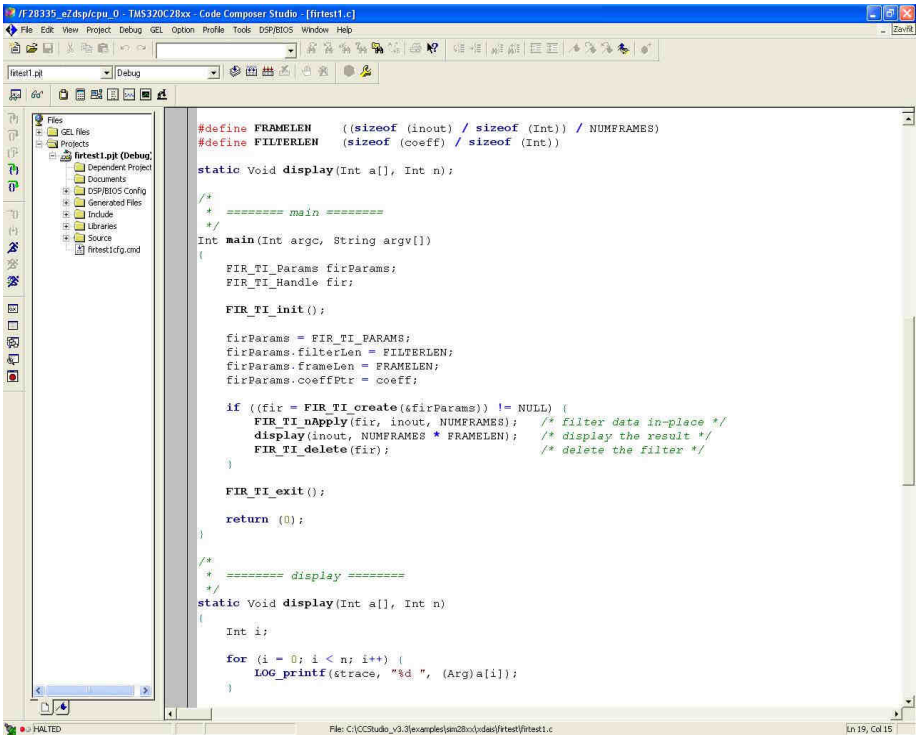
Tabulka 6.6 Jednotlivá stavová slova a jejich význam

7 Softwarové řešení

Pro zvládnutí komunikace mezi řídicím mobilním systémem a osobním počítačem je nutné využít různá programovací prostředí. Počínaje prostředím pro programování systému se signálovým procesorem, konče vývojovým prostředím pro ovládání periferií osobního počítače a zajištění procesu sběru dat.

7.1 Systém se signálovým procesorem

Zde je použito Code Composer Studio, které vytváří prostor k programování systému se signálovým procesorem. Umožňuje zápis zdrojových programů, jak v jazyce symbolických adres, tak také v jazyce C. V tomto prostředí probíhá i odlazování programů a překlad do strojového kódu. Využití vyšších programovacích jazyků výrazně urychluje implementaci algoritmů a zvyšuje přehlednost programu. Nevýhodou však je, že strojový kód generovaný ze zdrojových příkazů v jazyce C má většinou větší velikost i větší výpočetní náročnost, než strojový kód generovaný z asembleru. Základními programovými prostředky pro získání strojového kódu jsou překladač jazyka C, překladač jazyka signálového procesoru a sestavovací program. Na obrázku 7.1 je znázorněno ovládací prostředí Code Composer Studia.



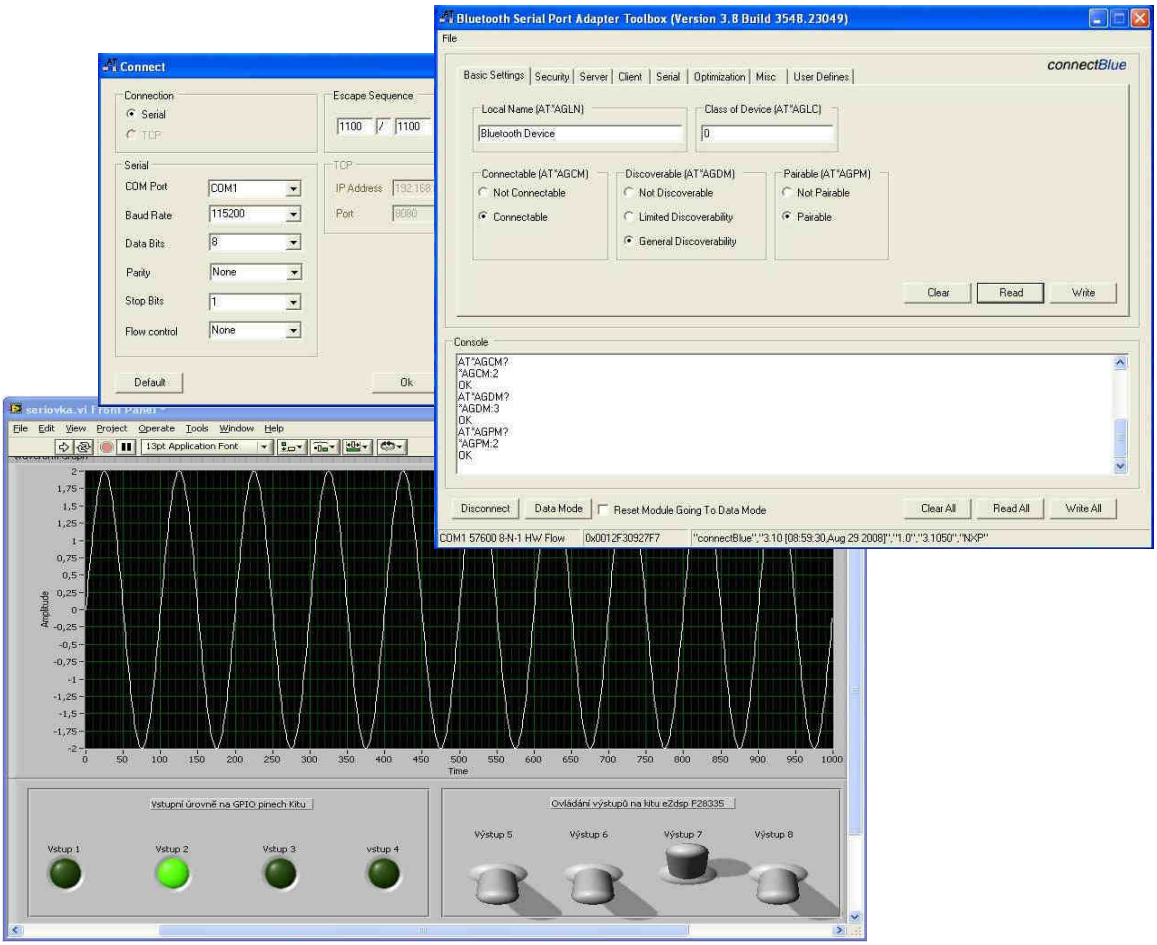
Obrázek 7.1 Prostředí Code Composer Studio

7.2 Počítač pro sběr dat

Pro komunikaci s bezdrátovými moduly na osobním počítači je využito grafické programovací prostředí LabView, SPA Toolbox, iChip Configuration tools a Hyper Terminál pro obecnou komunikaci AT+i příkazy. Na obrázku 7.2 a 7.3 jsou znázorněny příklady ovládacích oken.

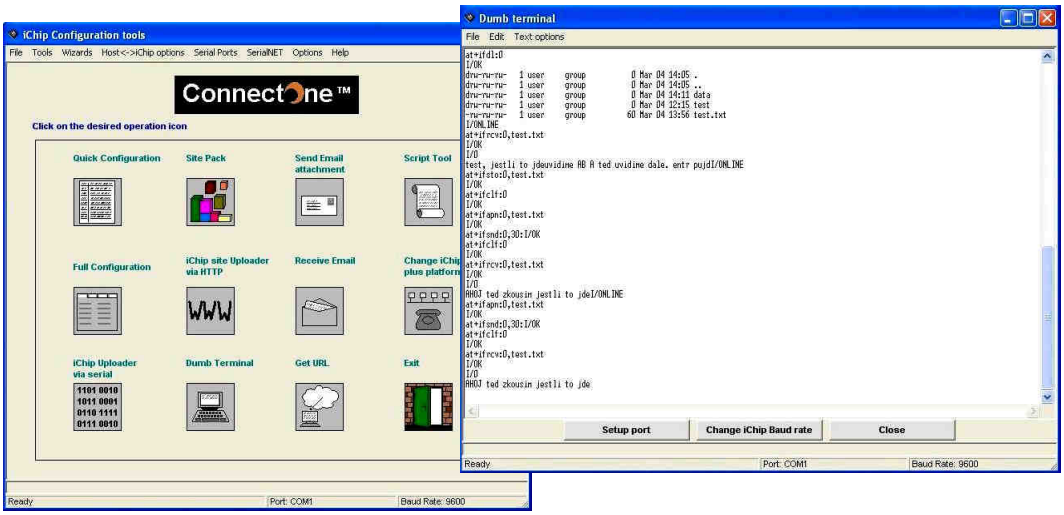
LabView je vývojové grafické prostředí vyvinuté společností National Instruments, které umožňuje práci v programovacím jazyce G. Jeho určením je tvorba aplikací pro řízení globálního procesu sběr, analýzy a následné prezentace dat. Toto prostředí je ve světě měřicí a řídicí techniky bráno jako standard, s nímž jsou srovnávány ostatní programy. Řada výrobců měřicích a řídicích systémů vyvíjí a dodává ke svým výrobkům knihovny, které usnadňují použití jejich výrobků právě při vytváření aplikací v tomto prostředí [37], [38].

SPA Toolbox pak zjednoduší prvotní konfiguraci bezdrátových Bluetooth modulů na osobním počítači. Je produktem firmy connectBlue, která vyrábí různé bezdrátové moduly. Kromě přímého vkládání AT příkazů umožňuje SPA Toolbox snadný zápis i čtení konfigurace modulů pomocí přednastavených hodnot. S moduly je komunikováno prostřednictvím RS232. Pokud není RS232 na PC k dispozici, je možné bez obtíží využít převodníku USB/RS232 [39].



Obrázek 7.2 Ovládací prostředí SPA Toolbox a LabView

iChip Configuration tools představuje prostředí pro komunikaci a nastavení WiFi modulů firmy ConnectOne. Pomocí AT+i příkazů je v Dumb terminálu možno konfigurovat moduly a navíc jsou k dispozici nástroje rychlé konfigurace založené na zapsání potřebných parametrů v graficko-textovém prostředí, umožňující zkrácení času prvotního nastavení. Taktéž je umožněna aktualizace firmwaru modulů díky utilitě iChip Uploader a to nejen pomocí dříve uloženého souboru s firmwarem, ale také online přes konfigurační web server modulu, je li povolen. Na obrázku 6.3 je znázorněno pracovní prostředí iChip Configuration tools spolu s otevřeným terminálem pro komunikaci prostřednictvím AT+i příkazů [40].



Obrázek 7.3 Ovládací prostředí iChip Configuration tools a Dumb terminál

Hyper Terminál je prostředí defaultně obsažené v operačním systému Windows XP. Je vyvolán v nabídce Start – Všechny programy – Příslušenství – Komunikace – Hyper Terminál. Umožňuje připojení k jiným zařízením a je využíván pro obecnou komunikaci s bezdrátovými moduly prostřednictvím AT+i příkazů. Čili pokud nejsou k dispozici softwarové nástroje jako SPA Toolbox, nebo iChip configuration tools, které mají vlastní prostředí pro AT+i komunikaci, může být použito Hyper Terminálu. Pro komunikaci s GSM/GPRS modulem MC55i není k dispozici žádné výrobcem dodané prostředí usnadňující konfiguraci, a tedy bude Hyper Terminál využit jako primární prostředí pro ověření vlastností, komunikace a nastavení.

Po ověření základních vlastností, komunikace a nastavení modulů s bezdrátovou technologií prostřednictvím nástrojů jmenovaných výše, byly hardwarové moduly propojeny s podpůrnou deskou a vyzkoušené algoritmy implementovány do procesoru na kitu eZdsp320F28335.

8 Experimentální výsledky

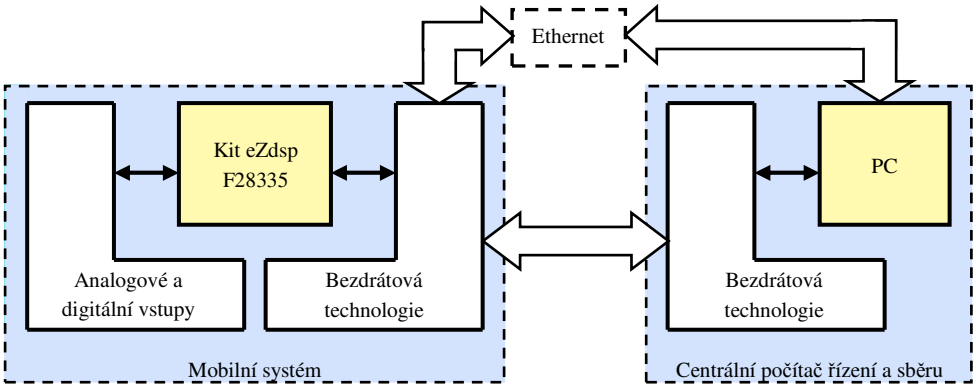
V této kapitole jsou popsány experimentální výsledky práce. Je zde naznačena struktura laboratorního pracoviště a ukázáno experimentální ověření přenosu dat prostřednictvím technologií Bluetooth, WiFi, GPRS.

Konkrétně je předvedena Bluetooth komunikace mezi vývojovým kitem eZdsp TMS320F28335 a personálním počítačem, případně Pocket PC pracujícím s operačním systémem Windows Mobile 6.5. Dále je naznačen přenos dat na FTP server s použitím technologie WiFi. Také je nakonfigurována a prakticky vyzkoušená Ad-Hoc WiFi síť pro přenos sériové linky mezi dvěma WiFi moduly se zabezpečením WEP. Následně je ukázáno odeslání kontrolní SMS uživateli při definovaných podmínkách. Další ukázkou je přenos dat z pracoviště pro bezsenzorové řízení asynchronních motorů s využitím infrastrukturního SerialNET přenosu se zabezpečením WPA2. Kapitola je ukončena aplikací monitorování spotřeby elektrické energie elektromobilu Tatra Beta s přenosem dat na FTP server prostřednictvím technologie GPRS.

8.1 Laboratorní pracoviště

Laboratorní pracoviště se skládá z mobilního systému a centrálního počítače, určeného k řízení a sběru dat z mobilního systému. Na obrázku 8.1 je znázorněna bloková struktura laboratorního pracoviště.

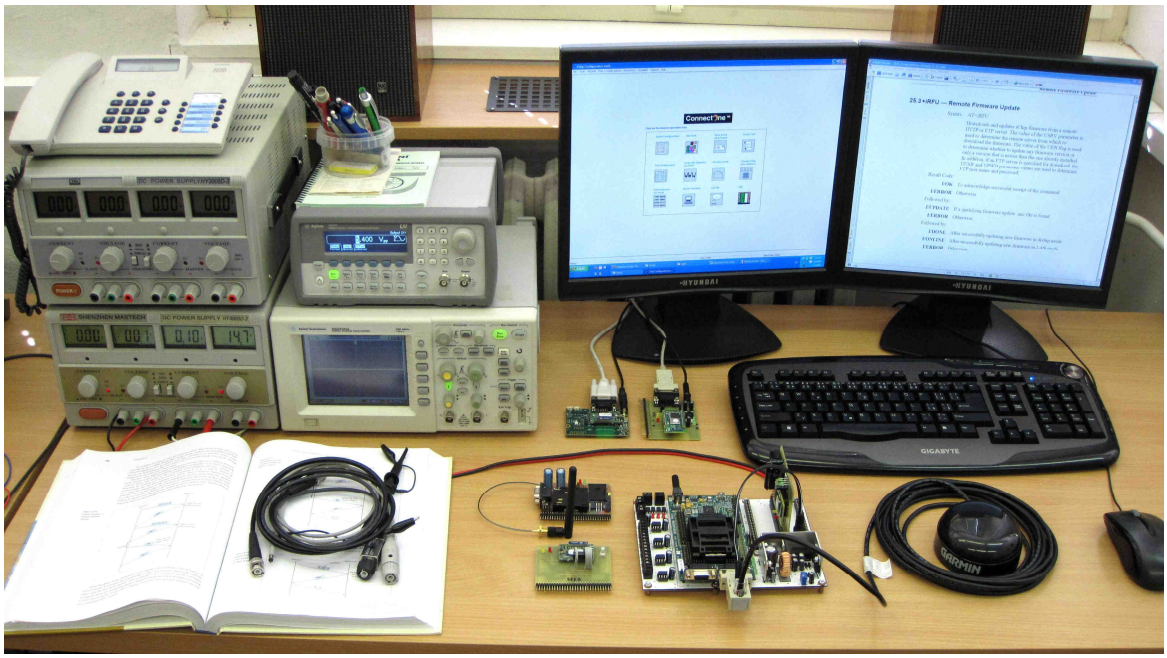
Mobilní systém obsahuje periferie pro komunikaci s okolím, jako jsou analogové vstupy, nebo digitální vstupy a výstupy. Vývojový kit eZdsp TMS320F28335 pak tyto periferie koordinuje a následně pomocí bezdrátové technologie odesílá centrálnímu počítači potřebná data. Bezdrátovou technologii je možné velice efektivně změnit pouhou výměnou bezdrátového modulu a rekonfigurací řídicího software.



Obrázek 8.1 Bloková struktura laboratorního pracoviště

Centrální počítač následně komunikuje pomocí zvolené bezdrátové technologie s mobilním systémem, umožňuje vizualizaci změřených dat, řízení celého procesu sběru dat a konfiguraci mobilního systému.

Pro dosažení nejvhodnější konfigurace mobilního systému a centrálního počítače je žádoucí mít k dispozici dostatečné spektrum mobilních technologií. Je to dáno tím, že jednotlivé aplikace mají svá specifika využití a to hlavně v oblasti prostorového využívání, okolního rušení a v neposlední řadě ekonomiky provozu. Proto je potřeba vždy vybrat vyhovující technologii přenosu. Jsou dostupné technologie Bluetooth, WiFi a GSM/GPRS. Na obrázku 8.2 je znázorněno laboratorní pracoviště.



Obrázek 8.2 Laboratorní pracoviště pro přenos dat

8.2 Experimentální ověření přenosu dat

Při konstrukcí mobilního systému je potřeba provést experimentální ověření funkce jednotlivých bloků. Jedná se hlavně o nastavení a komunikaci bezdrátových modulů s kitem eZdsp TMS320F28335. Taktéž je nutné ověřit obvodová zapojení bezdrátových modulů, bloků pro přizpůsobení úrovní signálů a v neposlední řadě také tvorbu obslužného softwarového vybavení osobního počítače a signálového procesoru TMS320F28335. V dalším textu je věnována pozornost jednotlivým experimentálním přenosům dat prostřednictvím dostupných technologií.

8.2.1 Přenos dat na PC prostřednictvím Bluetooth

V situacích kdy, je vyžadován přímý přenos dat na personální počítač, může být výhodné využití technologie Bluetooth a to nejen proto, že přenosné počítače (notebooky) mají stále častěji integrovanou technologii Bluetooth, ale také z důvodů snadné dostupnosti USB/Bluetooth modulů použitelných ve stolních počítačích a podobně. Pro laboratorní účely je však použit RS232/Bluetooth adaptér, umožňující velmi snadno sledovat provoz na RS232 lince. K tomu může být využit například Hyper Terminál dostupný přímo v operačním systému Windows XP.

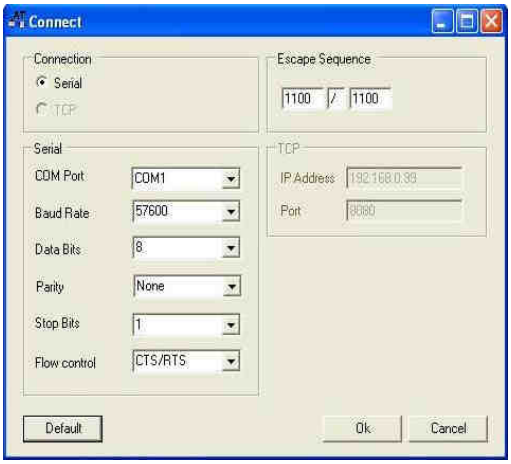
Pro experimentální přenos dat z mobilního systému na personální počítač pomocí Bluetooth technologie jsou nezbytné následující hardwarové bloky, které byly popsány v kapitole 6.4.

- Mobilní systém reprezentovaný podpůrnou deskou s integrovaným vývojovým kitem eZdsp TMS320F28335.
- Bluetooth rozšiřující deska s modulem OEM serial port adapter™ 312.
- OEM RS232 Module Adapter III s integrovaným bluetooth modulem OEM serial port adapter™ 312.

Před započetím přenosu je provedena základní konfigurace Bluetooth modulů. To může proběhnout zadáváním AT+i příkazů pomocí Hyper Terminálu, nebo je k tomu využito softwarového prostředí SPA Toolbox viz kapitola 7.2. Následně jsou moduly spárovány. Při nastavení bude jeden modul nakonfigurován jako Client a druhý jako Server, s tím, že pro následné využití bezdrátového přenosu nezáleží, který modul bude Client a který Server. Dále je uveden příklad základního nastavení pomocí konfiguračního prostředí SPA Toolbox pro modul Client. Po spuštění SPA Toolboxu je vybrán produkt Bluetooth SPA viz obrázek 8.3.

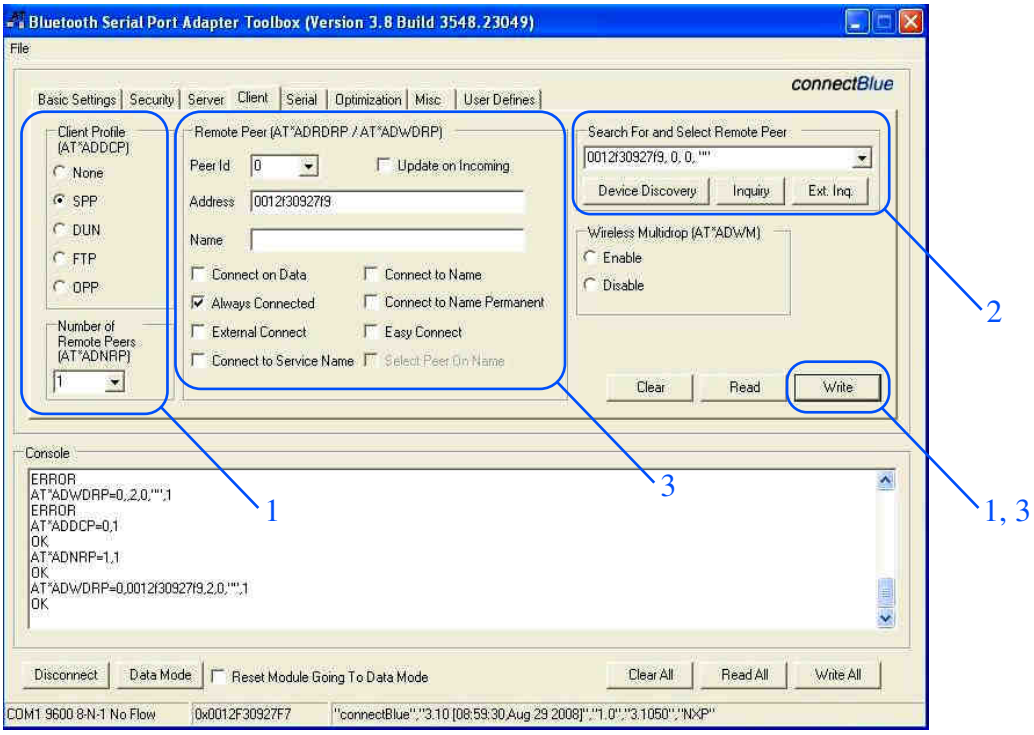
Obrázek 8.3 Výběr produktu Bluetooth SPA

Po stisknutí tlačítka OK se zobrazí okno, které v levém dolním rohu obsahuje tlačítko Connect. Po jeho aktivaci se zobrazí podokno nastavení komunikace. Defaultní konfigurace je zobrazena na obrázku 8.4. Je nutné vybrat správný COM Port, ke kterému je modul připojen, v tomto případě COM1. Parametry sériové komunikace mohou být později změněny na hodnoty definované uživatelem.



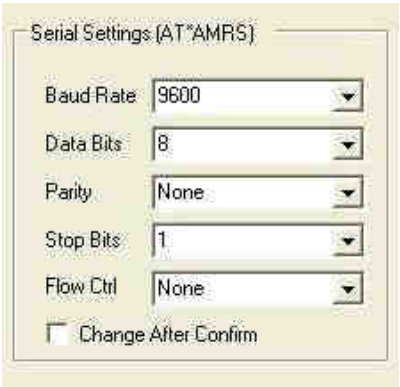
Obrázek 8.4 Nastavení komunikačního portu a sériové komunikace

Po vybrání volby AT Mode a přepnutí na záložku Client budou provedeny následující nastavení. Vybere se Client Profile – SPP a Number of Remote Peers – 1 a potvrdí tlačítkem Write. Následně se u druhého modulu zapne napájení a v menu Search For and Select Remote Peer se aktivuje volba Device Discovery. Po dokončení hledání dostupných zařízení se nastaví volba Peer Id – 0 a v roletkovém menu Search For and Remote Peer se vybere druhý modul. Tím se tento modul přenese do kolonky Address. Nyní se zatrhne Always Connected a změny zapíšou tlačítkem Write. Nastavení modulu Client ilustruje obrázek 8.5.



Obrázek 8.5 Nastavení modulu Client

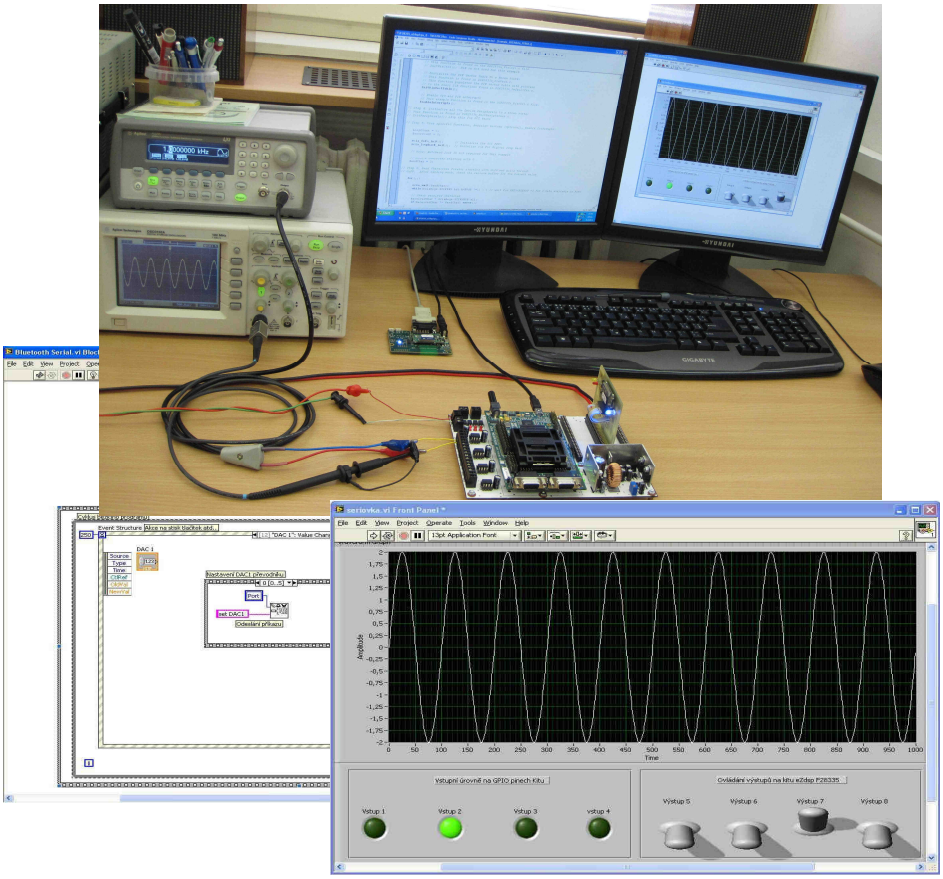
Jestliže sériové nastavení komunikace není vyhovující, je možná jeho změna v záložce Serial. Na obrázku 8.6 je podstatný výřez záložky Serial, kde je umožněno nastavení přenosové rychlosti, počtů přenášených datových bitů, nastavení parity, počet stop bitů a nastavení kontroly toku.



Obrázek 8.6 Konfigurace sériové komunikace

Pro nastavení druhého modulu do režimu Server není potřeba jakékoli nastavení, krom konfigurace parametrů RS232 respektive UART komunikace v případě, že nevyhovuje defaultní nastavení. Při změně tohoto nastavení se postupuje podobně, jako v předchozím textu.

Pomocí vytvořeného software v LabView na osobním počítači je umožněna bezdrátová komunikace prostřednictvím Bluetooth modulů s vývojovým kitem eZdsp TMS320F28335, jež má implementován obslužný program vytvořený v Code Composer Studiu. Na obrázku 8.7 je znázorněno experimentální pracoviště spolu s ovládacím panelem a náznakem blokového diagramu programovacího prostředí LabView.



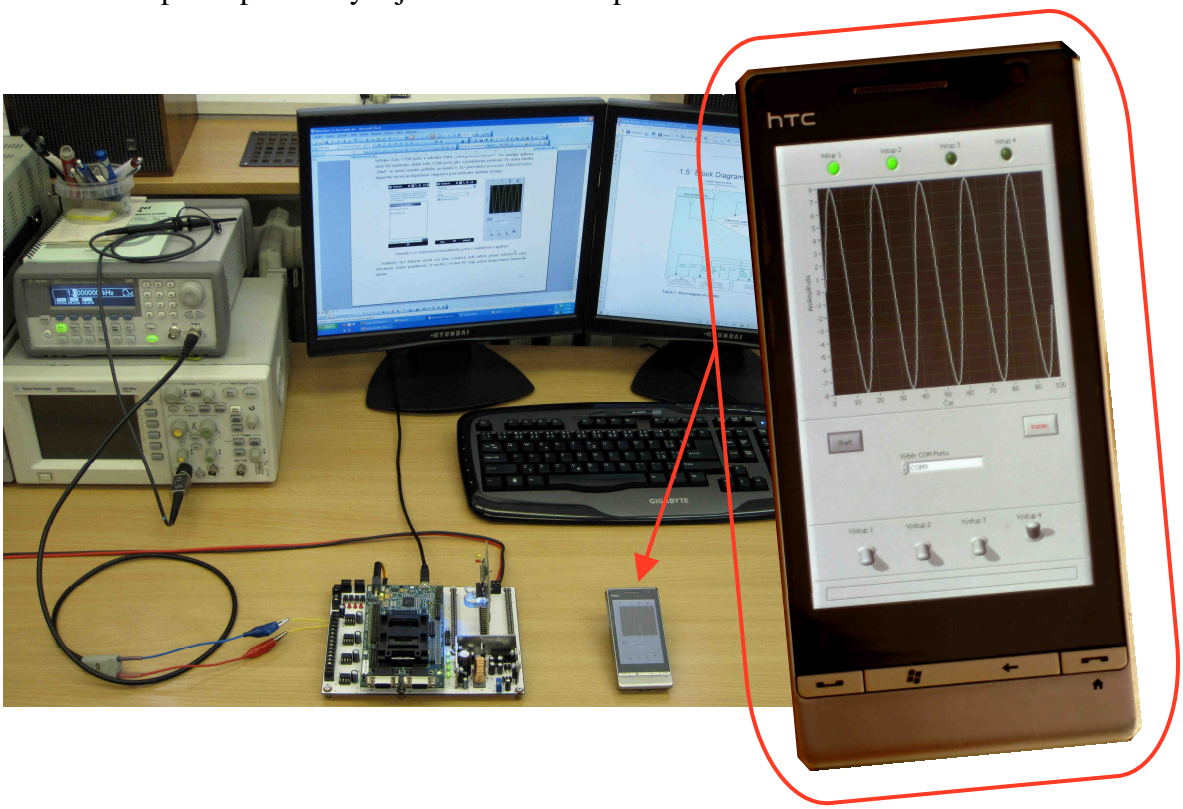
Obrázek 8.7 Pracoviště pro přenos dat prostřednictvím Bluetooth a ovládací panel

Ovládací program umožňuje grafické zobrazení průběhů na kanále 0 AD převodníku a také ovládání čtyř digitálních výstupů a snímání logické úrovně na čtyřech digitálních vstupech vývojového kitu.

Komunikace probíhá prostřednictvím SPP [11], jež definuje protokoly a postupy, používané u zařízení k emulaci sériového přenosu. Tím jsou vytvořeny virtuální sériové porty, jak na personálním počítači, tak i na vývojovém kitu eZdsp F28335. Iniciátorem, tedy zařízením inicializujícím připojení k jinému zařízení je kit, respektive jeho Bluetooth modul (Server) a akceptorem, který čeká na inicializující zařízení je personální počítač (Client).

8.2.2 Experimentální aplikace pro Pocket PC

Vzhledem k rostoucí dostupnosti a výpočetní výkonnosti Pocket PC a PDA se nabízí implementace algoritmů původně určených počítači pro sběr dat. Jako Pocket PC posloužil HTC Diamond 2, vybavený operačním systémem MS Windows Mobile 6.5. V programovacím prostředí LabView byla vytvořena aplikace komunikující s mobilním systémem prostřednictvím Bluetooth. Ovládací panel je zřejmý z obrázku 8.8. Umožňuje sledování průběhů na kanále 0 AD převodníku, dále ovládání výstupních pinů a sledování úrovní na vstupních pinech vývojového kitu eZdsp F28335.



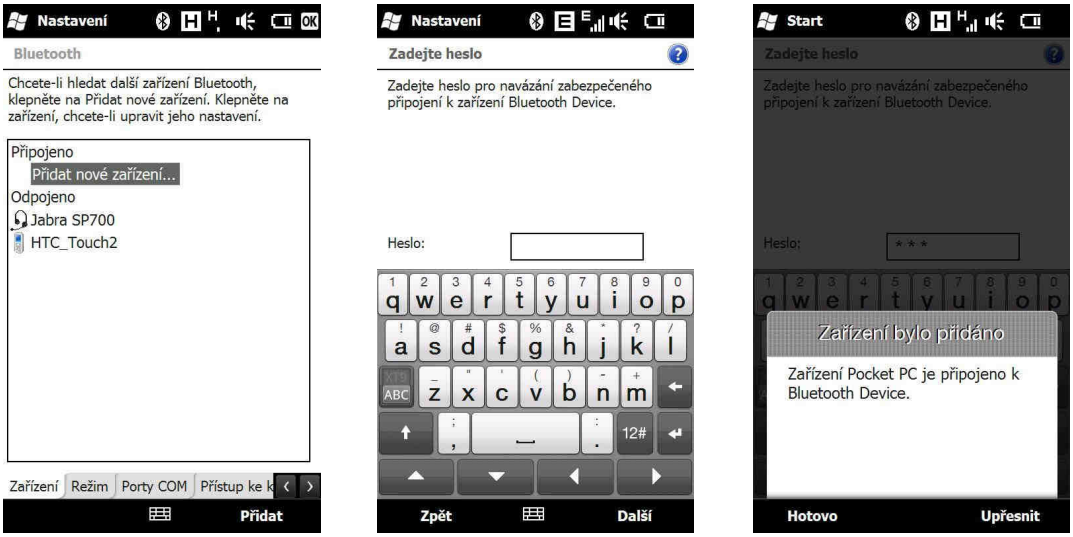
Obrázek 8.8 Komunikace kitu eZdsp s Pocket PC

Komunikace probíhá opět prostřednictvím SPP. Jsou vytvořeny virtuální sériové porty, jak na Pocket PC, tak i na vývojovém kitu eZdsp TMS320F28335. Iniciátorem je Pocket PC, konkrétně HTC Diamond (Client), a akceptorem (Server) je kit se signálovým procesorem který čeká na inicializující zařízení, respektive Bluetooth modul obsažený na rozšiřující desce.

Při realizaci tohoto přenosu dat je vhodné nastavit bezpečnostní prvky jako je autentizace, autorizace, případně i využít šifrování. K této konfiguraci je možno použít opět Hyper Terminál, nebo softwarové prostředí SPA Toolbox.

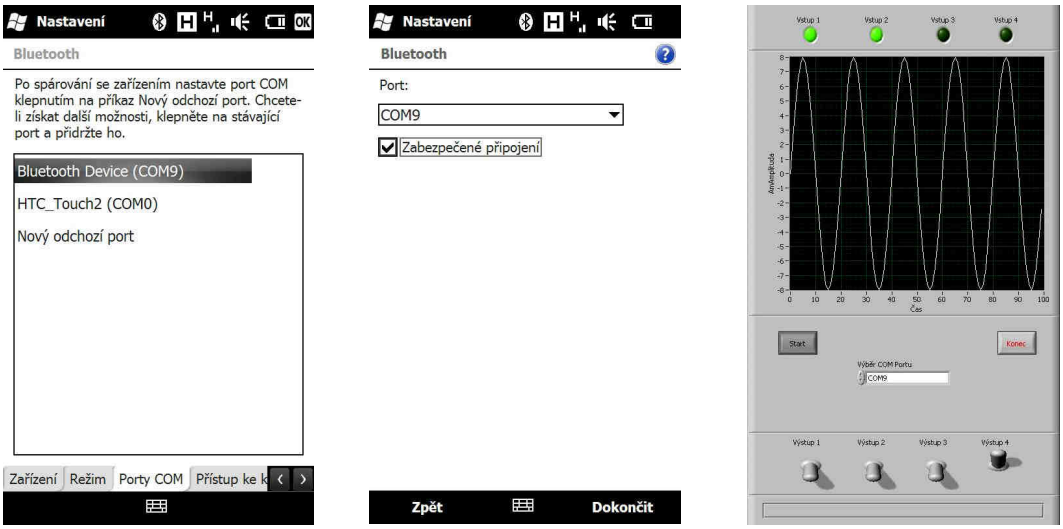
Pro názornost jsou dále znázorněny ukázky obrazovek smartphonu při párování zařízení a nastavení virtuálního komunikačního portu. Na obrázku 8.9 jsou obrazovky z průběhu párování. Po aktivaci hledání nového zařízení se zobrazí seznam dostupných Bluetooth zařízení. Je vybráno zařízení Bluetooth Device. Jakmile je zadáno správné heslo k provedení

zabezpečeného připojení k zařízení Bluetooth Device, ukáže se hláška, že zařízení Pocket PC je připojeno k Bluetooth Device.



Obrázek 8.9 Párování Bluetooth modulu s HTC Diamond 2

Nyní je potřeba nastavit COM port v Pocket PC pro komunikaci prostřednictvím SPP. Vybere se volba „Nový odchozí port“ a označí zařízení Bluetooth Device. Následně je vybráno číslo COM portu a zatržena volba „Zabezpečené připojení“. Po spuštění aplikace vytvořené opět v LabView a zkompilované pro Windows Mobile 6.5 musí být nastaveno stejné číslo COM portu jako v předchozím nastavení. Po stisku tlačítka „Start“ se spustí snímání průběhu na kanále 0 AD převodníku procesoru TMS320F28335, skenování úrovní na digitálních vstupech a jsou nastaveny digitální výstupy.



Obrázek 8.10 Nastavení komunikačního portu v smartphonu a aplikaci

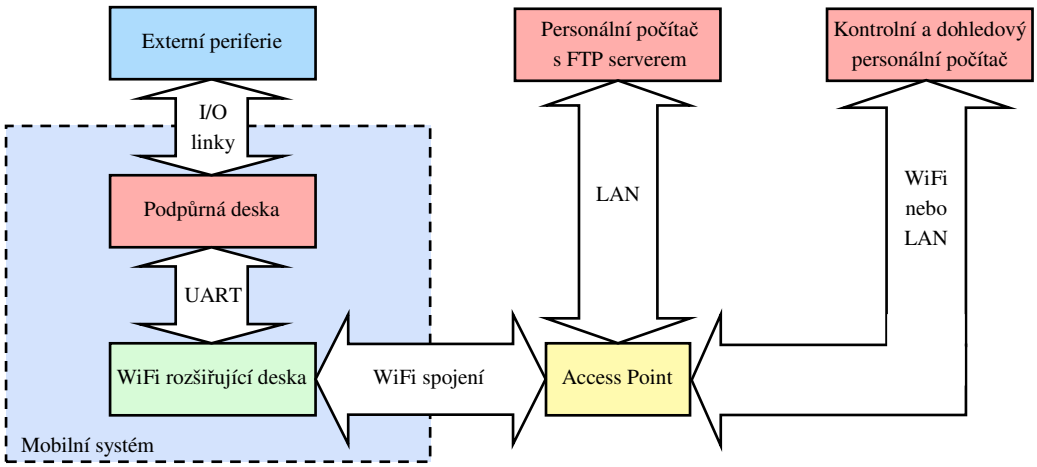
Prakticky byl dokázán dosah cca 30m v budově, kde nebyla přímá viditelnost mezi zařízeními. Nutno podotknout, že modul i Pocket PC mají pouze integrovanou Bluetooth anténu.

8.2.3 Přenos dat prostřednictvím WiFi na FTP server

FTP neboli File Transfer Protocol je služba umožňující práci se vzdálenými soubory. Podporuje stahování nebo nahrávání souborů na vzdálený server, jakožto i mazání souborů, práci s adresáři, změnu přístupových práv atd. Služba je využita k přenosu souborů z mobilního zařízení na FTP server, kde budou data následně využita k zpracování a vizualizaci. K sestavení experimentálního pracoviště jsou potřebné následující hardwarové moduly.

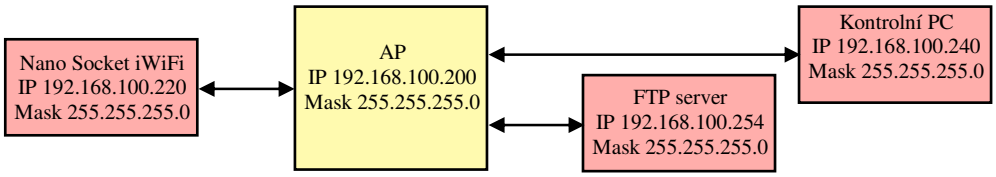
- Mobilní systém reprezentovaný podpůrnou deskou s integrovaným vývojovým kitem eZdsp TMS320F28335.
- WiFi rozšiřující deska s modulem Nano Socket iWiFi.
- Access Point, v tomto případě Air Live Wireless AP - WL5450-AP.
- FTP server spuštěný na personálním počítači.

Struktura pracoviště je naznačena na obrázku 8.11. Mobilní systém komunikující s externími periferiemi odesílá data prostřednictvím WiFi rozšiřující desky na FTP server. Jako prostředník mezi komunikací je Access Point. Ten vytváří rozhraní mezi WiFi a LAN, do nějž je připojen FTP server. K FTP serveru je možné se také přihlásit kontrolním a dohledovým personálním počítačem prostřednictvím LAN nebo WiFi. Tak je umožněn vzdálený dohled nad ukládanými daty z celé takto vytvořené sítě.



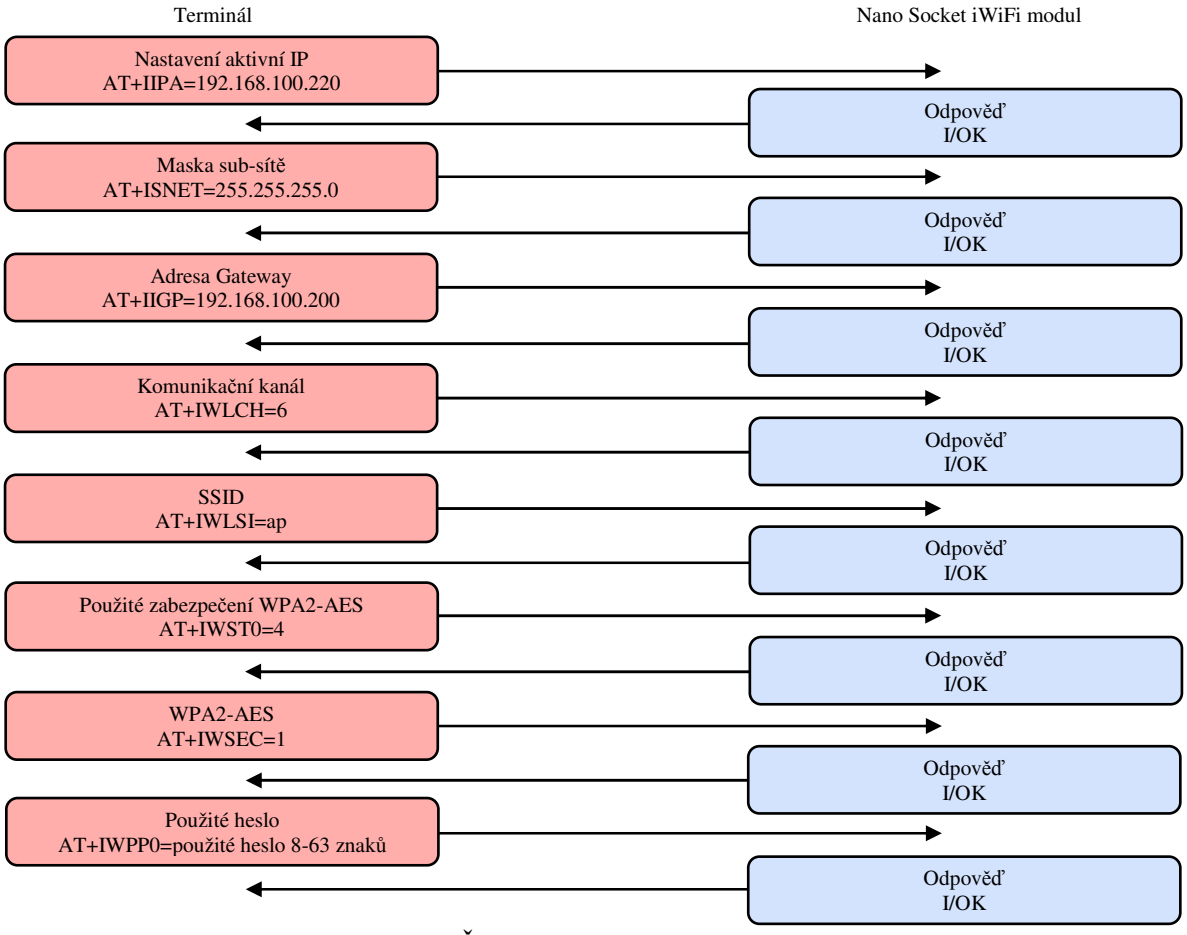
Obrázek 8.11 Struktura experimentálního pracoviště pro přenos dat na FTP

Před zahájením komunikace je potřeba celou síť nastavit. Byla vybrána konfigurace s pevnými IP adresami jednotlivých zařízení. Jednotlivé IP adresy prezentuje obrázek 8.12. Nastavení Access Pointu se provádí přes integrovaný konfigurační web server. Síťové karty personálních počítačů uživatel nastaví prostřednictvím softwaru integrovaného v operačním systému těchto počítačů.



Obrázek 8.12 IP adresy experimentální sítě

Konfigurace Nano Socket iWiFi modulu probíhá zasláním AT+i příkazů. Je možno také využít utilitu iChip Config, avšak nastavení AT+i příkazy se jeví jako přehlednější. Část průběhu konfigurace je znázorněn na obrázku 8.13. Ke komunikaci s ostatními zařízeními jsou podstatné parametry, jako aktivní IP adresa (AT+IIPA), maska sub-sítě (AT+ISNET), IP adresa Gateway (AT+IIPG), komunikační kanál (AT+IWLCH), SSID Access Pointu (AT+IWLSI) a další, včetně použitého zabezpečení, zde konkrétně WPA2-AES.

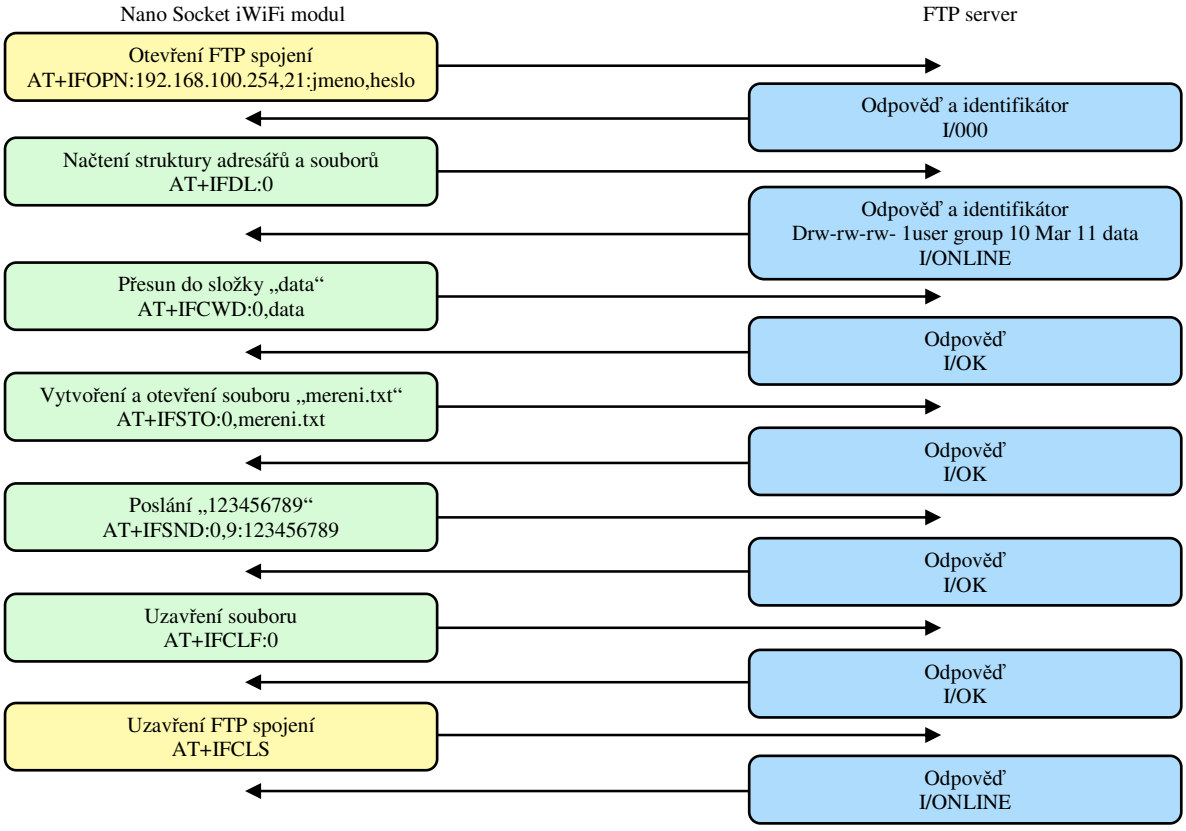


Obrázek 8.13 Část průběhu konfigurace modulu

Pro připojení k FTP serveru je využito pasivního FTP spojení a přenosu v ASCI módu. Před otevřením spojení zašle klient přihlašovací údaje (jméno a heslo) a číslo portu, na kterém bude komunikace probíhat na adresu FTP serveru. Server zašle odpověď, že je jméno a heslo správné a následuje otevření spojení. Nyní má klient umožněny operace na FTP serveru v rámci svých práv. Po dokončení operací na FTP serveru je potřeba uzavřít spojení a server potvrdí ukončení spojení.

WiFi modul má implementovanou podporu FTP. Komunikace mezi kitem eZdspTMS320F28335 a Nano Socket iWiFi modulem pobíhá prostřednictvím AT+i příkazů, které umožňují provádět následující operace na FTP serveru [41].

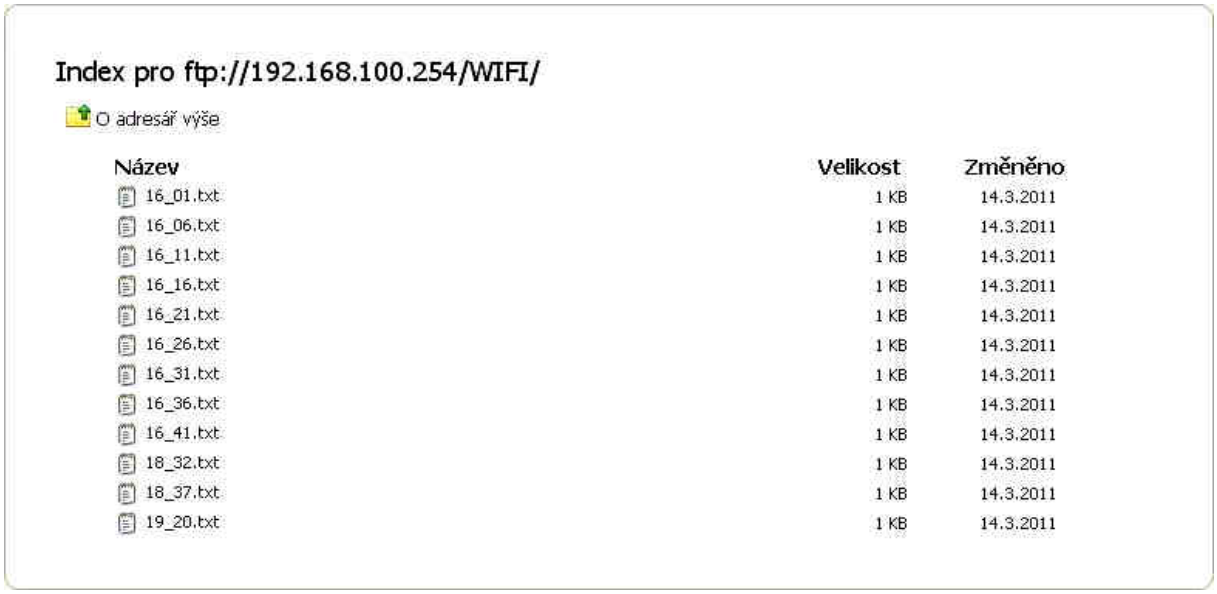
- Otevření FTP spojení (AT+IFOPN).
- Načtení souborové a adresářové struktury (AT+IFDL, AT+IFDNL).
- Změnu aktuální složky (AT+IFCWD).
- Načtení obsahu souboru (AT+IFRCV).
- Vytvoření nové složky (AT+IFMKD).
- Otevření nebo vytvoření nového souboru (AT+IFSTO).
- Otevření existujícího souboru pro úpravy (AT+IFAPN).
- Zaslání binárních dat do otevřeného souboru (AT+IFSND).
- Uzavření souboru po předchozím zápisu (AT+IFCLF).
- Smazání souboru (AT+IFDEL).
- Uzavření FTP spojení (AT+IFCLS).



Obrázek 8.14 Zjednodušená komunikace mezi klientem a FTP serverem

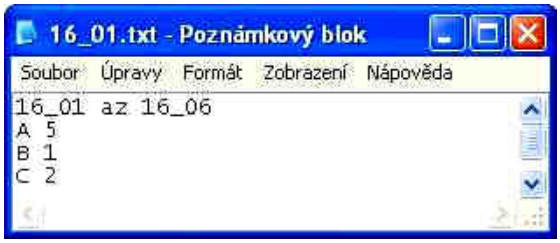
Na obrázku 8.14 je znázorněn příklad komunikace mezi klientem a serverem. Po otevření spojení (AT+IFOPN) FTP server pošle identifikátor, který je nutný při celé komunikaci do ukončení spojení. Tento identifikátor určuje pořadové číslo spojení, aby v případě přístupu na FTP server více uživateli, tito mohli být rozlišeni. Následně je načtena souborová a adresářová struktura (AT+IFDL), jsou zobrazeny práva k jednotlivým souborům a složkám, počet připojených uživatelů a datum poslední změny. Po přesunu do složky „data“ (AT+IFCWD) je vytvořen soubor s názvem „mereni.txt“ (AT+IFSTO). Dále jsou zaslána data „123456789“ (AT+IFSND). Tento příkaz obsahuje také pole, ve kterém je uložen počet znaků, které budou vysílány. Pak je soubor uzavřen po předchozím zápisu (AT+IFCLF). Následuje uzavření FTP spojení (AT+IFCLS) [41].

Příklady vytvořených datových souborů na FTP serveru jsou na obrázku 8.15. Byly odeslány datové bloky, ve kterých jsou informace o změnách stavů vstupních signálů, a o čase, kdy tyto změny nastaly. Soubory reprezentují pěti-minutové intervaly. Bylo celkem vytvořeno 12 souborů. Formát datové zprávy je znázorněn na obrázku 8.16.



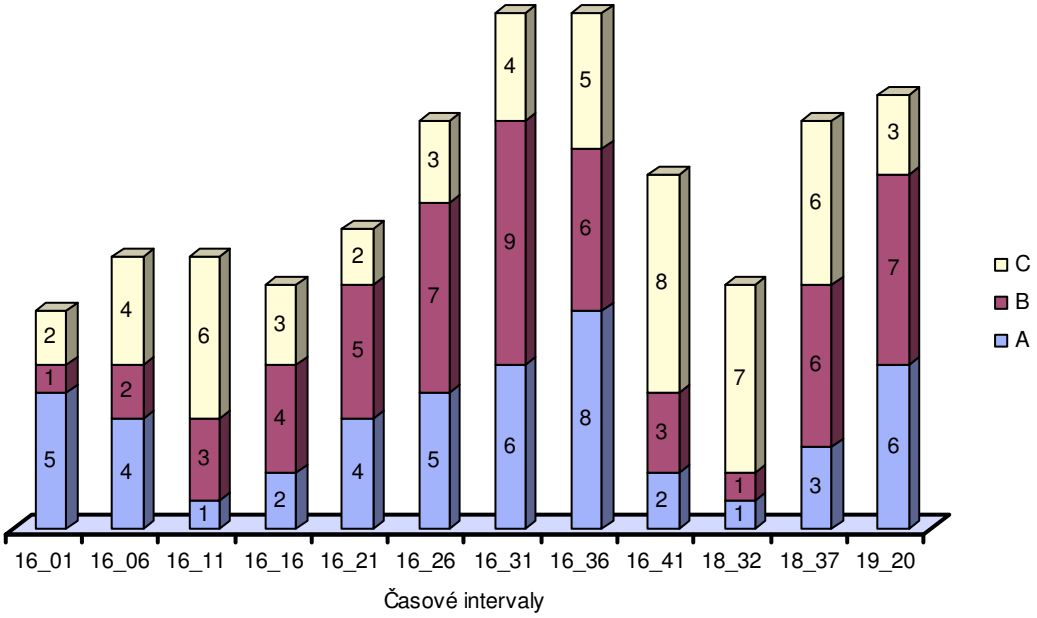
Obrázek 8.15 Odeslaná data na FTP server

Data je možné zpracovat například do grafu na obrázku 8.17, kde je znázorněna závislost četnosti změn logických úrovní vstupů A, B, C v časových intervalech. Modře je předvedena četnost změn na vstupu A, fialově pak na vstupu B a žlutě na vstupu C.



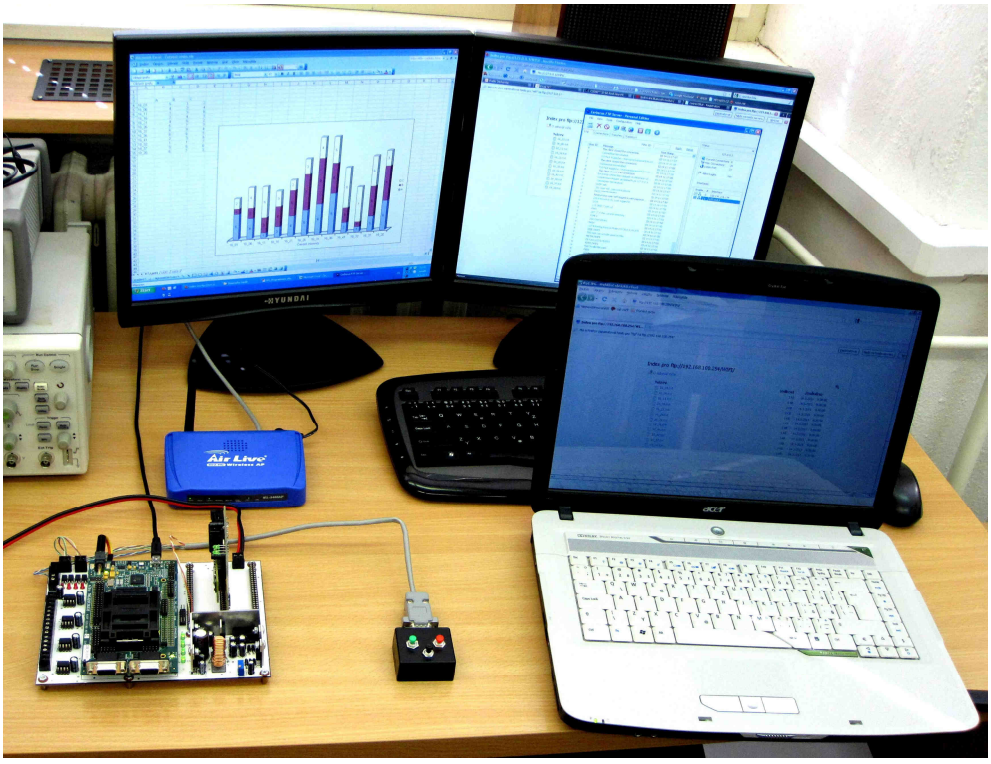
Obrázek 8.16 Formát experimentální datové zprávy

Je zřejmé, že odesílaná data na FTP server mohou reprezentovat širokou škálu informací. Počínaje údaji o poloze mobilního zařízení, přes informace o aktuálním stavu zařízení, nebo také naměřené veličiny a podobně. Systém přenosu dat na FTP server je tedy naprosto univerzální, co se týče využití v praxi.



Obrázek 8.17 Graf závislosti četnosti změn logických úrovní vstupů na časových intervalech

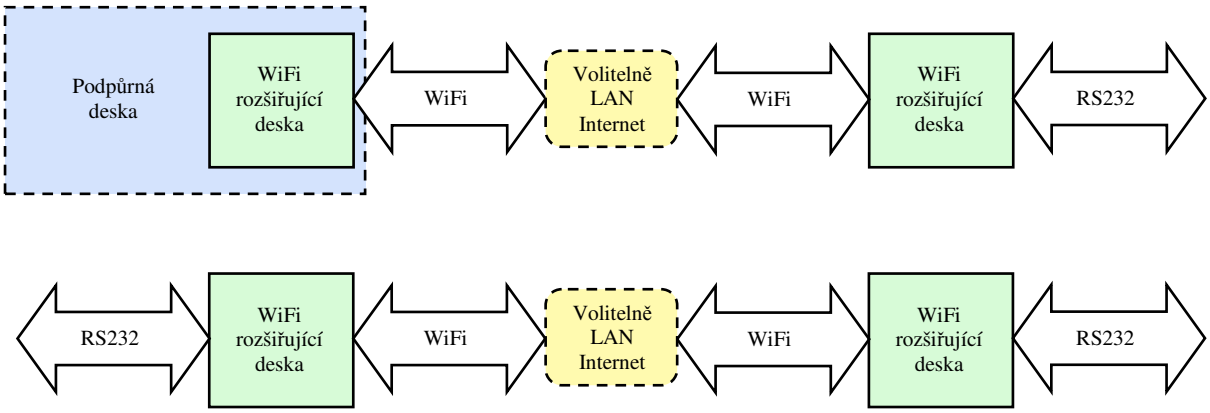
Data byla vyčtena při experimentálním propojení řídicího kitu eZdsp TMS320F28335 s WiFi modulem Nano Socket iWiFi, které je znázorněno na obrázku 8.18.



Obrázek 8.18 Experimentální přenos dat na FTP server

8.2.4 WiFi SerialNET

Pokud nastane potřeba bezdrátové náhrady RS232 linky, je možnost mimo Bluetooth využít také síť WiFi. Využívá se k tomu provozní režim SerialNET, který sadou AT+i příkazů umožňuje převod sériových dat na TCP/IP pakety. Tento režim nevyžaduje změny na hostitelském zařízení. Takto je umožněno prodloužení místní asynchronní sériové linky přes LAN nebo Internet, prakticky kamkoli. Za tímto účelem byl definován soubor parametrů, definující povahu požadované sítě. Pokud je WiFi modul Nano Socket iWiFi nastaven do režimu SerialNET, chová se jako směrovač mezi zařízením se sériovým portem a sítí. Když zařízení (client) iniciuje komunikaci, musí režim SerialNET navázat síťové spojení se vzdáleným serverem ještě před tím, než začnou proudit data mezi systémy. Jinak řečeno, režim SerialNET obsahuje postupy řízení přenosu dat mezi clientem a serverem. Tím je zajištěna plně duplexní trasa mezi terminály obou zařízení [42].



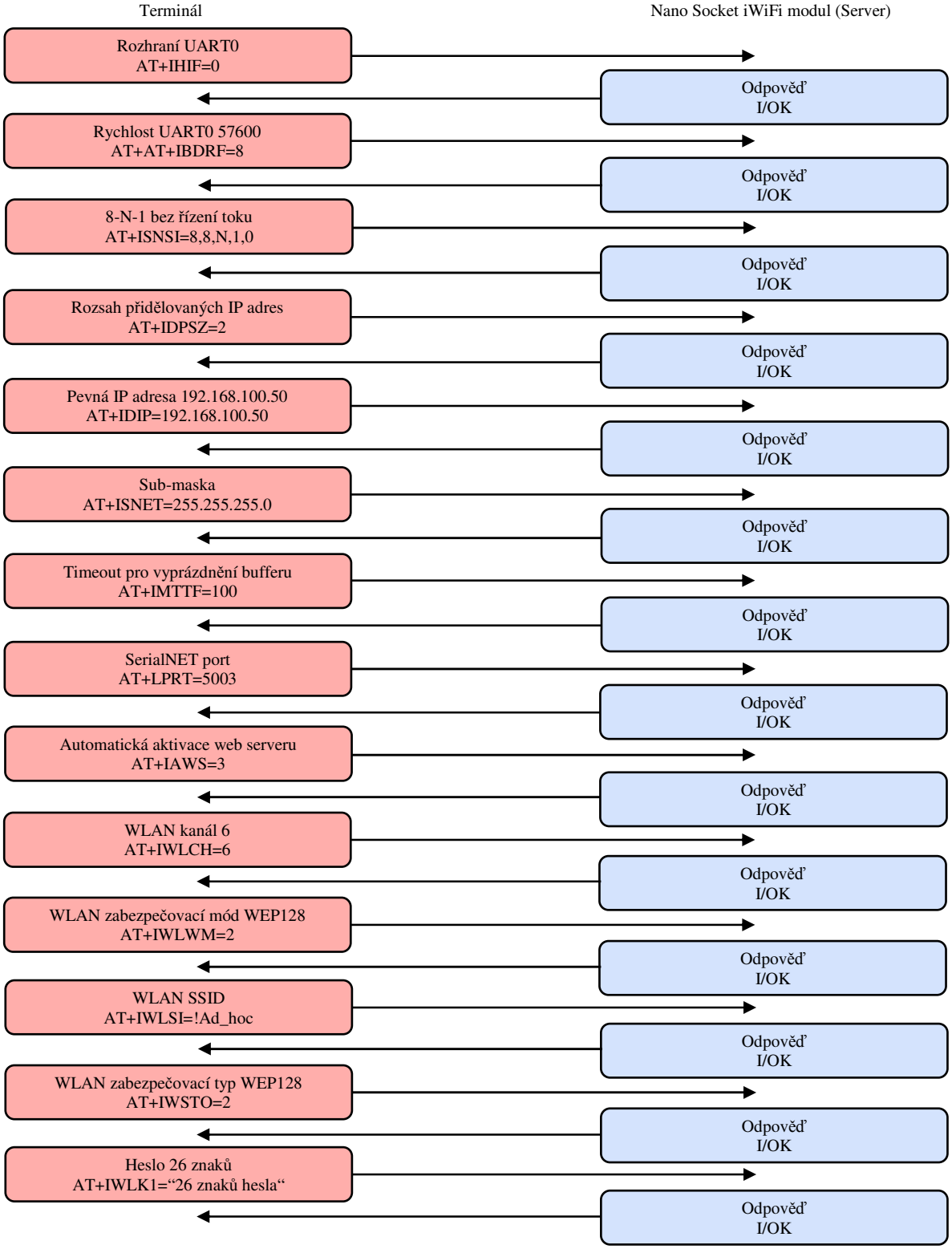
Obrázek 8.19 Možné zapojení WiFi rozšiřujících desek

Proto byly rozšiřující WiFi desky vybaveny přímou konektibilitou s RS232. Na obrázku 8.19 jsou znázorněny možné způsoby zapojení WiFi rozšiřujících desek. Jak již samotný obrázek naznačuje, k vytvoření WiFi Ad – hoc sítě bude potřeba následujících hardwarových modulů.

- Mobilní systém reprezentovaný podpůrnou deskou s integrovaným vývojovým kitem eZdsp TMS320F28335 (volitelně).
- WiFi rozšiřující deska s modulem Nano Socket iWiFi ve dvou kusech.

Konfigurace může být opět provedena dvěma způsoby. Buď pomocí Hyper Terminálu anebo pomocí software iChip Config. Pro názornost bude dále věnována pozornost konfiguraci prostřednictvím Hyper Terminálu. Nutnou podmínkou je, aby byl jeden modul nastaven jako Server a druhý jako Client. Dále při prvotní konfiguraci, můžou být na obou modulech spuštěny konfigurační web servery, které umožní pozdější rekonfiguraci přes webová rozhraní.

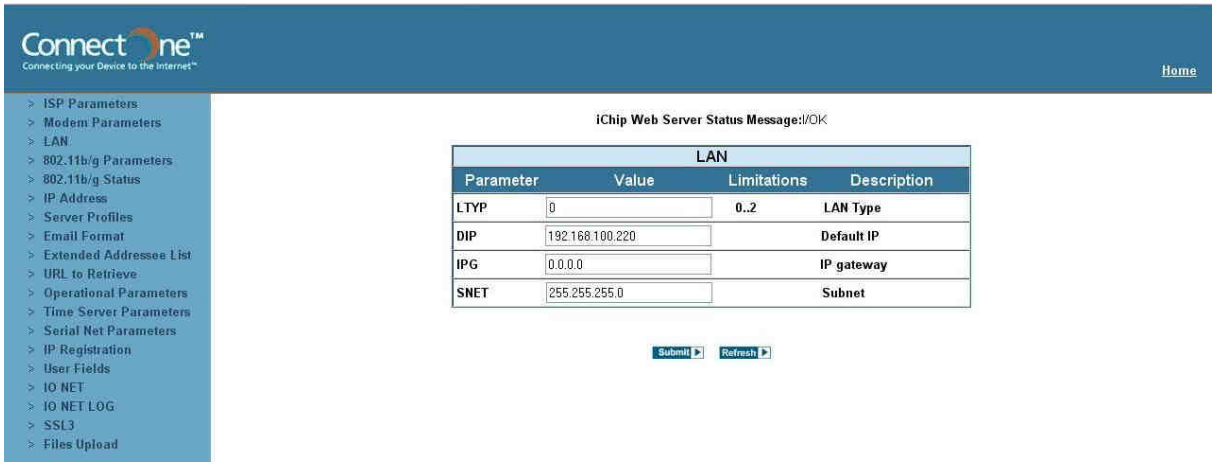
Modul Server bude mít následující vzorovou konfiguraci. Aktivní DHCP server (umožní přidělení dvou IP adres), pevnou IP adresu (192.168.100.50), aktivovaný konfigurační web server (192.168.100.50/ichip), SSID: Ad_hoc, zabezpečení WEP128, nastavení sériové linky (57600 kBit·s^{-1}, 8 datových bitů, bez parity, jeden stop bit, bez řízení toku). Obrázek 8.20 zobrazuje konfiguraci prostřednictvím AT+i příkazů modulu Server.



Obrázek 8.20 Vzorová konfigurace modulu Server

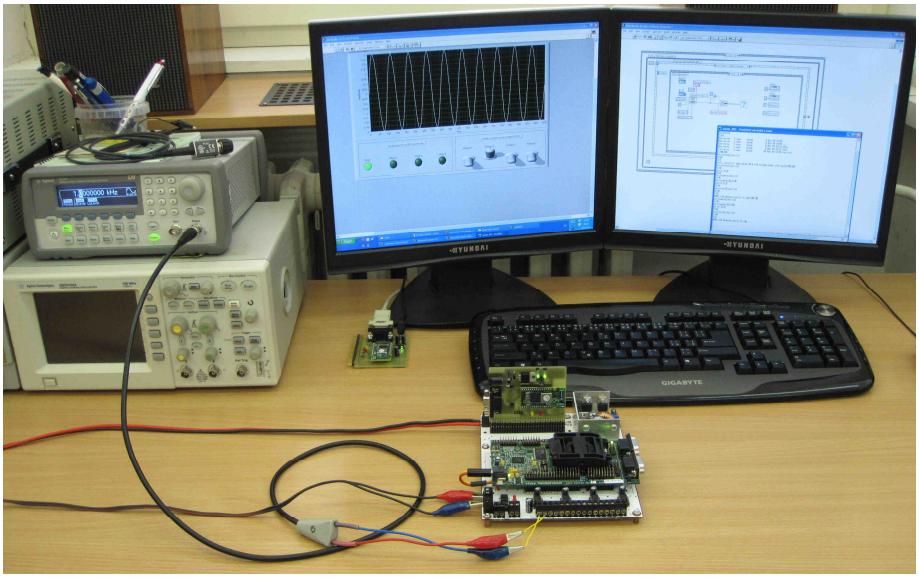
Modul Client bude mít aktivní DHCP client, také aktivní konfigurační web server obvykle na IP adrese (192.168.100.51/ichip), SSID: Ad_hoc, zabezpečení také WEP128, a stejné nastavení sériové linky jako u modulu Server. Konfigurace probíhá velice podobně jako u modulu Server na obrázku 8.20.

Konfigurační web server umožňuje celkovou správu modulu, tedy rekonfiguraci prakticky všech parametrů, nahrání aktuálního firmware apod. Dále je také podporována možnost vytvořit si sadu vlastních AT+i příkazů. Na obrázku 8.21 je ovládací panel konfiguračního web serveru. Přístup je z aktuální IP adresy modulu/ichip, například: http://192.168.100.50/ichip.



Obrázek 8.21 Příklad konfiguračního web serveru

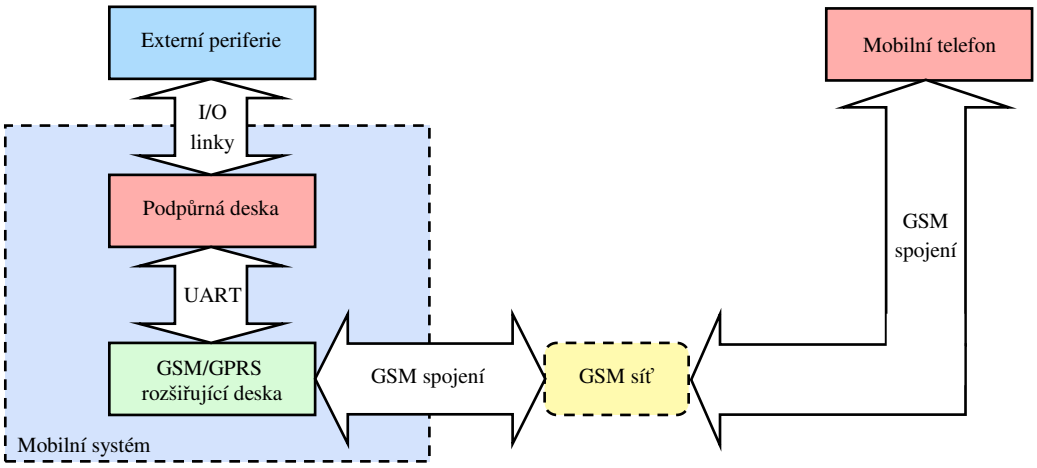
Experimentální pracoviště (obrázek 8.22) bylo přizpůsobeno online přenosu dat z mobilního systému reprezentovaného podpůrnou deskou s integrovaným kitem eZdsp TMS320F28335 a WiFi rozšiřující deskou. Data byla odesílána na další WiFi rozšiřující desku propojenou s personálním počítačem prostřednictvím RS232. Takto vzniklá síť využívá topologie Ad – hoc. Pro vizualizaci bylo použito ovládací prostředí původně vytvořené pro přenos dat prostřednictvím technologie Bluetooth.



Obrázek 8.22 Experimentální přenos dat prostřednictvím SerialNET

8.2.5 GSM SMS

Vzhledem k tomu, že dnes je prakticky každý vybaven GSM konektivitou v podobě mobilního telefonu, nabízí se možnost zasílání stavových SMS zpráv mobilního zařízení vzdálenému uživateli, případně může uživatel pomocí konfigurační SMS ovlivnit funkci zařízení. Výhodou tohoto řešení je, že uživatel krom mobilního telefonu nemusí disponovat dalšími nadstavbovými moduly, ani technologiemi. Mobilní zařízení případně jiný systém, který má být monitorován případně konfigurován se vybaví GSM modulem a jeho řízení následně obstará procesor v konkrétní aplikaci. Na obrázku 8.23 je ukázáno zjednodušené blokové schéma sestavy pro odesílání SMS z mobilního zařízení vzdálenému uživateli.

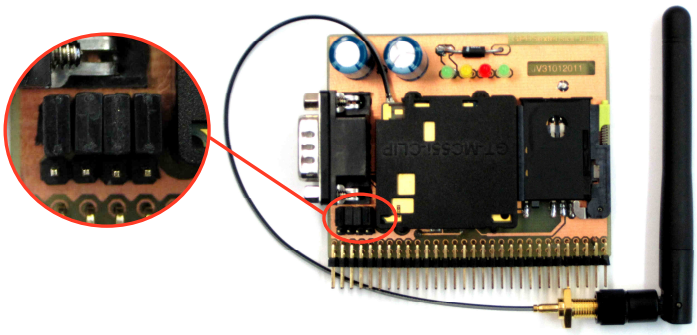


Obrázek 8.23 Bloková sestava pro odesílání SMS z mobilního zařízení vzdálenému uživateli

K vytvoření experimentálního pracoviště pro odesílání SMS budou nutné níže uvedené hardwarové moduly.

- Mobilní systém reprezentovaný podpůrnou deskou s integrovaným vývojovým kitem eZdsp TMS320F28335.
- GSM/GPRS rozšiřující deska s aktivní kartou SIM.
- Mobilní telefon pro příjem SMS.

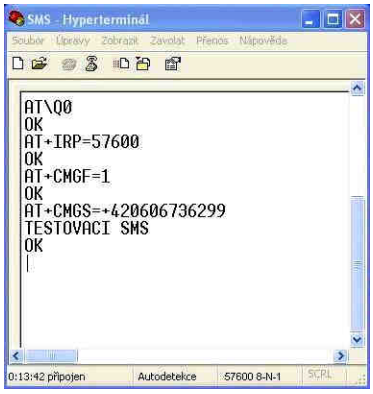
Po instalaci karty SIM do GSM/GPRS rozšiřující desky je vhodné nejdřív ověřit komunikaci a funkci pomocí Hyper Terminálu. Rozšiřující deska se zasune do podpůrné desky a provede se konfigurace RS232 propojkami viz obrázek 8.24. SCI propojky zůstanou neosazeny. Tím se přesměruje komunikační kanál na konektor Canon 9. K dispozici je tak RS232 linka včetně hardwarového řízení toku. Propojení je provedeno přímým kabelem se sériovým COM portem personálního počítače. Jakmile se zapne napájení podpůrné desky je GSM/GRPS rozšiřující deska respektive její modul MC55i připraven přijímat AT+i příkazy z Hyper Terminálu. Modul MC55i se nyní nachází v režimu automatického přizpůsobení komunikační rychlosti.



Obrázek 8.24 Nastavení konfiguračních propojek GSM/GPRS rozšiřující desky pro komunikaci prostřednictvím konektoru Canon 9

Základní nastavení sériové linky je provedeno na komunikační rychlost 57,6 kbit·s^{-1} (AT+IPR=57600) a bez softwarového a hardwarového řízení toku (AT/Q0). Takto bude také následně komunikovat vývojový kit eZdsp TMS320F28335, respektive jeho procesor prostřednictvím podpůrné a rozšiřující desky s modulem MC55i.

Jakmile je za použití Hyper Terminálu otestováno přihlášení do sítě (AT+CREG=?) je odeslána testovací SMS zpráva. To je ilustrováno výřezem z Hyper Terminálu na obrázku 8.25. Ještě před odesláním je nutné nastavit, že SMS bude odeslána v textovém módu (AT+CMGF=1).



Obrázek 8.25 Výřez Hyper Terminálu při odesílání SMS

Registraci do sítě a další informace o stavu modulu MC55i lze také zjistit pohledem na status LED. V tabulce 8.1 jsou znázorněny možné stavy modulu v závislosti na svitu status LED.

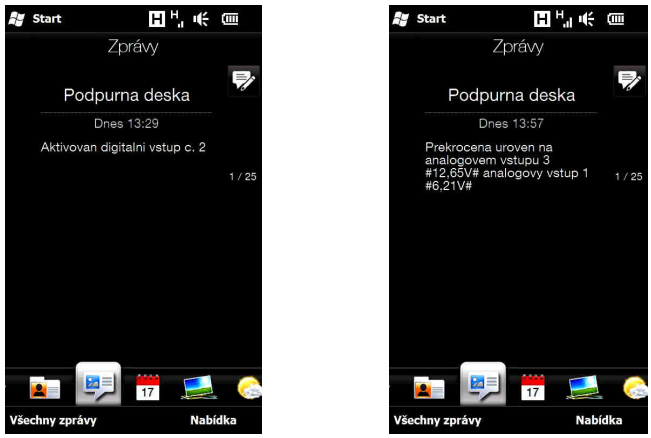
Status LED	Stav modulu MC55i
Stále nesvítí	Power down mód, Alarm mód, Cyclic sleep mód,
600 ms svítí / 600 ms nesvítí	Omezené síťové služby (chybí SIM, chybný PIN, přihlašování k síti)
75 ms svítí / 3 s nesvítí	Idle mód (modul připojen k síti, nekoná se žádný hovor)
75 ms svítí / 75 ms nesvítí / 75 ms svítí / 3 s nesvítí	GPRS aktivní
0,5 s svítí / nesvítí při přenosu dat	LED se rozsvítí na 1 s, až jsou datové pakety přeneseny
Stále svítí	Při probíhajícím hlasovém nebo CSD hovoru

Tabulka 8.1 Dekódování stavů modulu dle status LED

Modul MC55i umožňuje odesílat a přijímat SMS, dále podporuje ukládání přijatých SMS do paměti, vytváření seznamu vlastních předdefinovaných SMS a jejich odesílání a celkovou správu SMS [34].

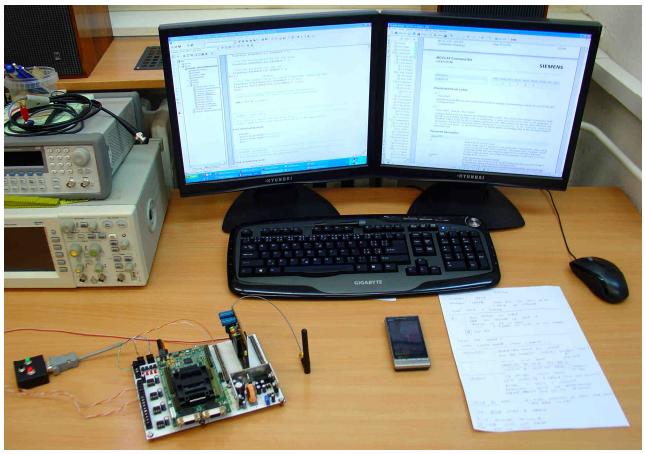
Pro mobilní systém reprezentovaný podpůrnou deskou, vývojovým kitem eZdsp TMS320F28335 a GSM/GPRS rozšiřující deskou byl vytvořen software, umožňující odeslat informační SMS po překročení napěťové úrovně 10 V na analogovém vstupu číslo 1 a 3 podpůrné desky, nebo při aktivaci minimálně jednoho ze čtyř samostatných digitálních vstupů. Informační SMS pak zobrazí, na kterém analogovém vstupu byla překročena úroveň a jaká jsou napětí na obou vstupech, případně který digitální vstup byl aktivován.

V případě reakce na aktivaci digitálních vstupů byly vytvořeny předdefinované SMS a ty uloženy v paměti modulu. Ty lze pomocí příkazu AT+CMSS odeslat pouhým vložením indexu a telefonního čísla. U reakce na překročení úrovně na analogových vstupech je situace odlišná a text SMS je vytvořen přímo v procesoru vývojového kitu eZdsp TMS320F28335. Na obrázku 8.26 je ukázán displej mobilního telefonu po příchodu informačních SMS.



Obrázek 8.26 Displej mobilního telefonu po příchodu informační SMS

K otestování přenosu SMS bylo sestaveno experimentální laboratorní pracoviště znázorněné na obrázku 8.27.

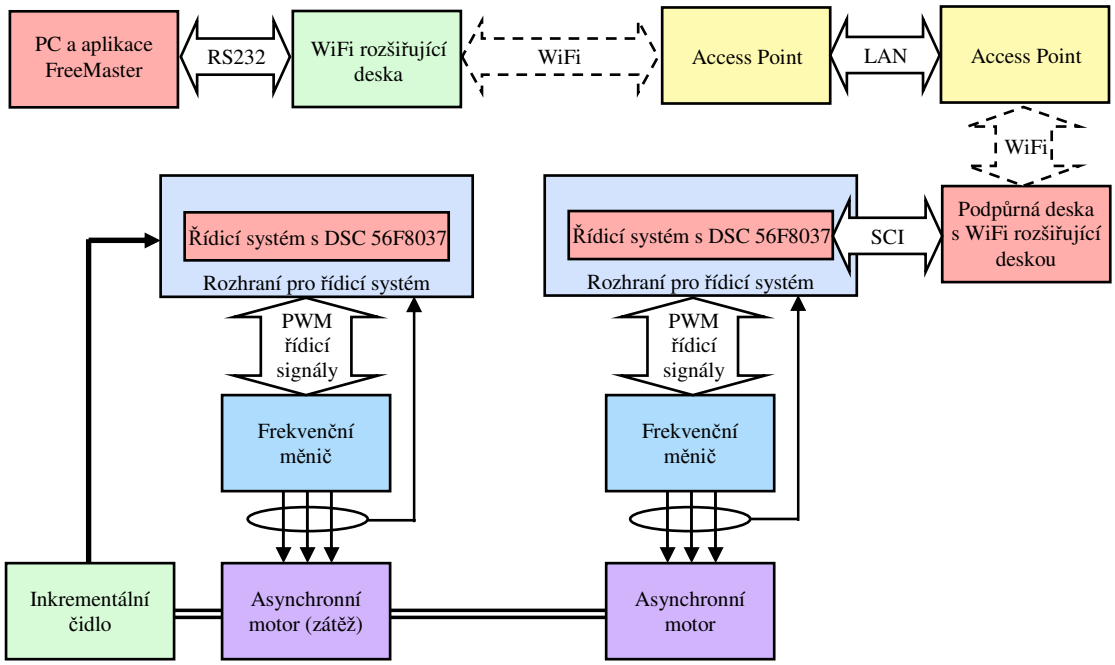


Obrázek 8.27 Experimentální pracoviště odesílání informačních SMS

8.2.6 Přenos dat z pracoviště pro bezsenzorové řízení asynchronních motorů

Bezsenzorové metody řízení pohonů neeliminují veškerá čidla, avšak pouze snímače osazené na hřídeli stroje, měřící polohu a rychlost rotoru. Tyto snímače jsou přídavné mechanické prvky a mohou do jisté míry degradovat dobré vlastnosti pohonu. Proto jsou vyvíjeny bezsenzorové metody, které zlepšují parametry pohonu a jeho spolehlivost a také snižují jeho cenu [43].

Pro aplikaci bezdrátové komunikace pohonu s asynchronními motory a softwarového prostředí FreeMaster, což je monitor veličin v reálném čase a grafický ovládací panel, byl vybrán WiFi infrastrukturní přenos prostřednictvím režimu SerialNet. Pracoviště se skládá ze soustrojí dvou vzájemně propojených asynchronních motorů o jmenovitém výkonu 2,2 kW a inkrementálního čidla, kde je jeden motor využit jako zátěž pro motor druhý, ovládaný bezsenzorovými metodami. Dále dvou výkonových polovodičových měničů kmitočtu s IGBT tranzistory, dvou rozhraní pro řídicí systém a dvou řídicích systémů s DSC Freescale 56F8037. Tento DSC disponuje potřebným množstvím periferií, dostatečnou pamětí a výpočetním výkonem pro aplikace bezsenzorových metod. Bloková struktura laboratorního pracoviště je znázorněna na obrázku 8.28.

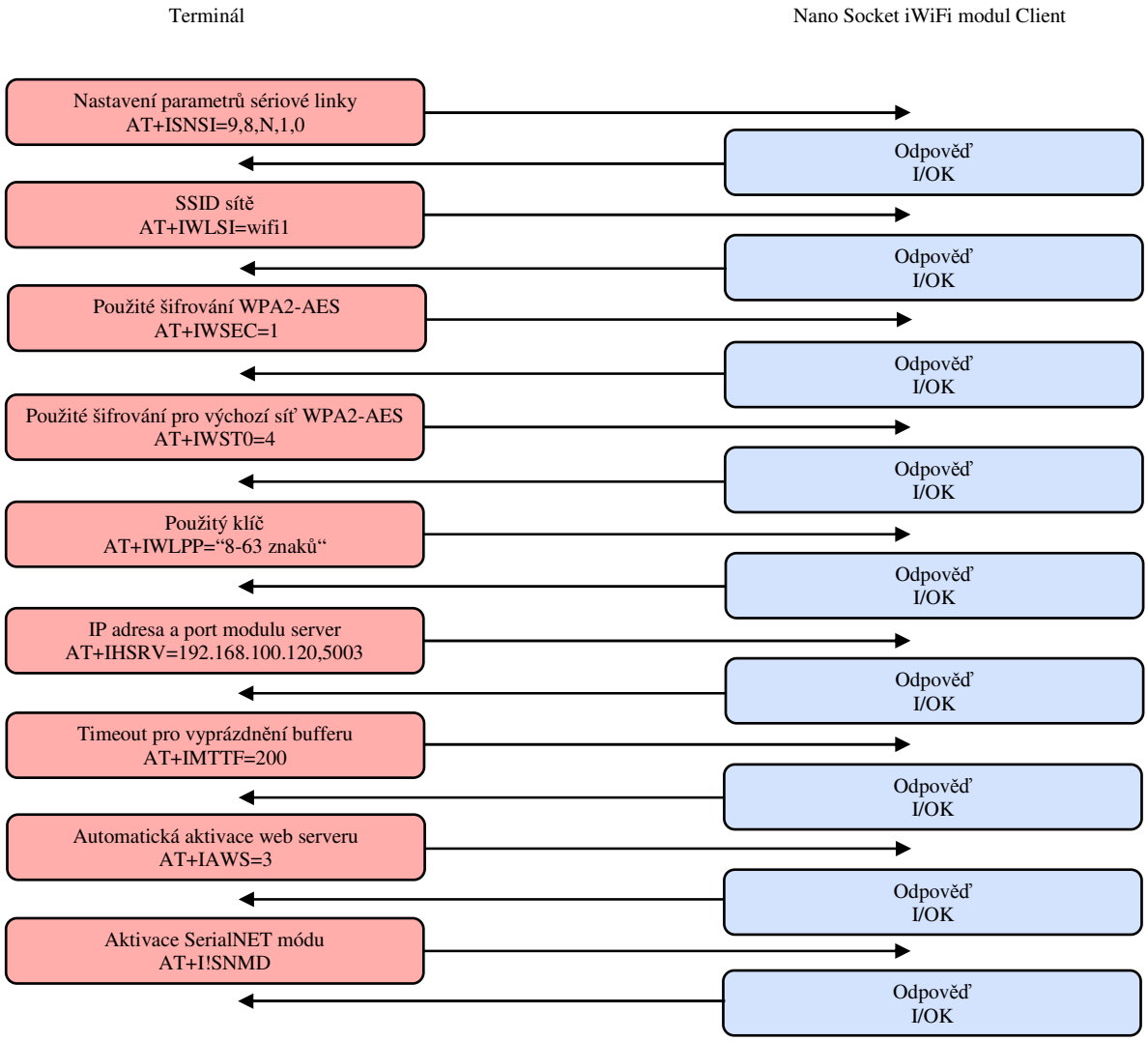


Obrázek 8.28 Bloková struktura laboratorního pracoviště

Jak již bylo napsáno, je pro komunikaci využit WiFi infrastrukturní přenos dat v režimu SerialNET. Ten se liší od Ad-hoc přenosu popsaného v kapitole 8.2.4 tím, že je umožněno ovládání a přenos dat prakticky z jakéhokoli umístění s konektibilitou k LAN. Je to dáno připojením Access Pointů do lokální sítě.

Použití infrastrukturní sítě má také výhodu v možnosti využití zabezpečení WPA/WPA2, které není v případě Ad-hoc k dispozici. To umožní prakticky neprolomitelný přenos dat, v případě použití dostatečně silného klíče.

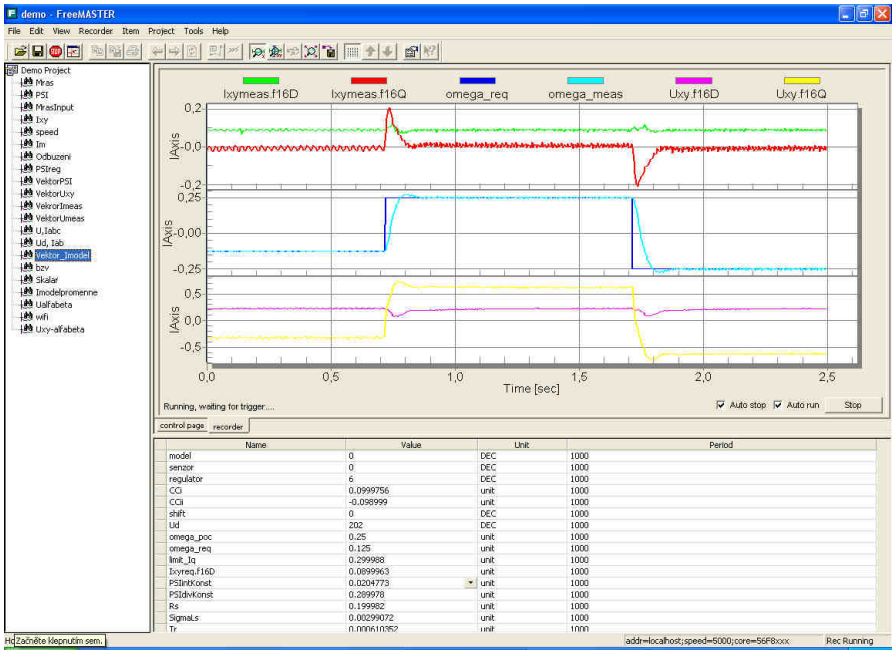
Konfigurace modulů Client a Server probíhá podobně jako v kapitole 8.2.4 s tím rozdílem, že se nastaví SSID WiFi sítě ke které bude modul připojen (AT+IWLSI), dále použité šifrování (AT+IWSEC) a (AT+IWST0) na WPA2-AES, vloží se heslo (AT+IWLPP), IP adresa serveru v případě, že Client zahájí aktivní spojení (AT+IHSRV) a pak se spustí SerialNET mód, který zůstane spuštěn i po opětovném připojení modulů k napájecímu napětí. Parametry sériové komunikace jsou nastaveny na 115200 $bit \cdot s^{-1}$ bez řízení toku a bez parity. Na obrázku 8.29 jsou znázorněna rozdílná nastavení modulu Client oproti síti Ad-hoc.



Obrázek 8.29 Přídavná nastavení pro infrastrukturní síť a modul Client

Tato nastavení lze provést pomocí AT+i příkazů, případně prostřednictvím spuštěného konfiguračního web serveru, nebo také v prostředí iChip Configuration tools. Vzhledem k implementaci nastavovacích algoritmů i do řídicího procesoru TMS320F28335 nebyly tyto grafické nadstavby využity ani u konfigurace samotného modulu komunikujícího s aplikací FreeMaster a bylo výhradně používáno AT+i příkazů.

Softwarové prostředí FreeMaster (obrázek 8.30) umožňuje vzdálené ovládání řídicího systému s procesorem Freescale 56F8037 přímo z osobního počítače. Zobrazení proměnných případně jejich změna probíhá v reálném čase a to jak v grafické, tak i textové podobě. Je umožněn také export vybraných parametrů do textového souboru a mnoho dalších funkcí.



Obrázek 8.30 Softwarové prostředí FreeMaster

Pro ilustraci byla exportována data ze dvou měření, která byla následně zpracována v tabulkovém procesoru Microsoft Excel. Ukázka exportovaného textového souboru s názvem „rec2.txt“ je znázorněna na obrázku 8.31. Data jsou řazena ve sloupcích a oddělena tabulátorem. Jednotlivé sloupce jsou uvozeny názvem, usnadňujícím pozdější orientaci v datech. V konkrétním příkladu je zaznamenán čas, žádané otáčky motoru, žádaná hodnota tokotvorného a momentotvorného napětí v orientovaném souřadném systému (x, y) a žádaná hodnota tokotvorného a momentotvorného napětí v statorovém souřadném systému (α, β).

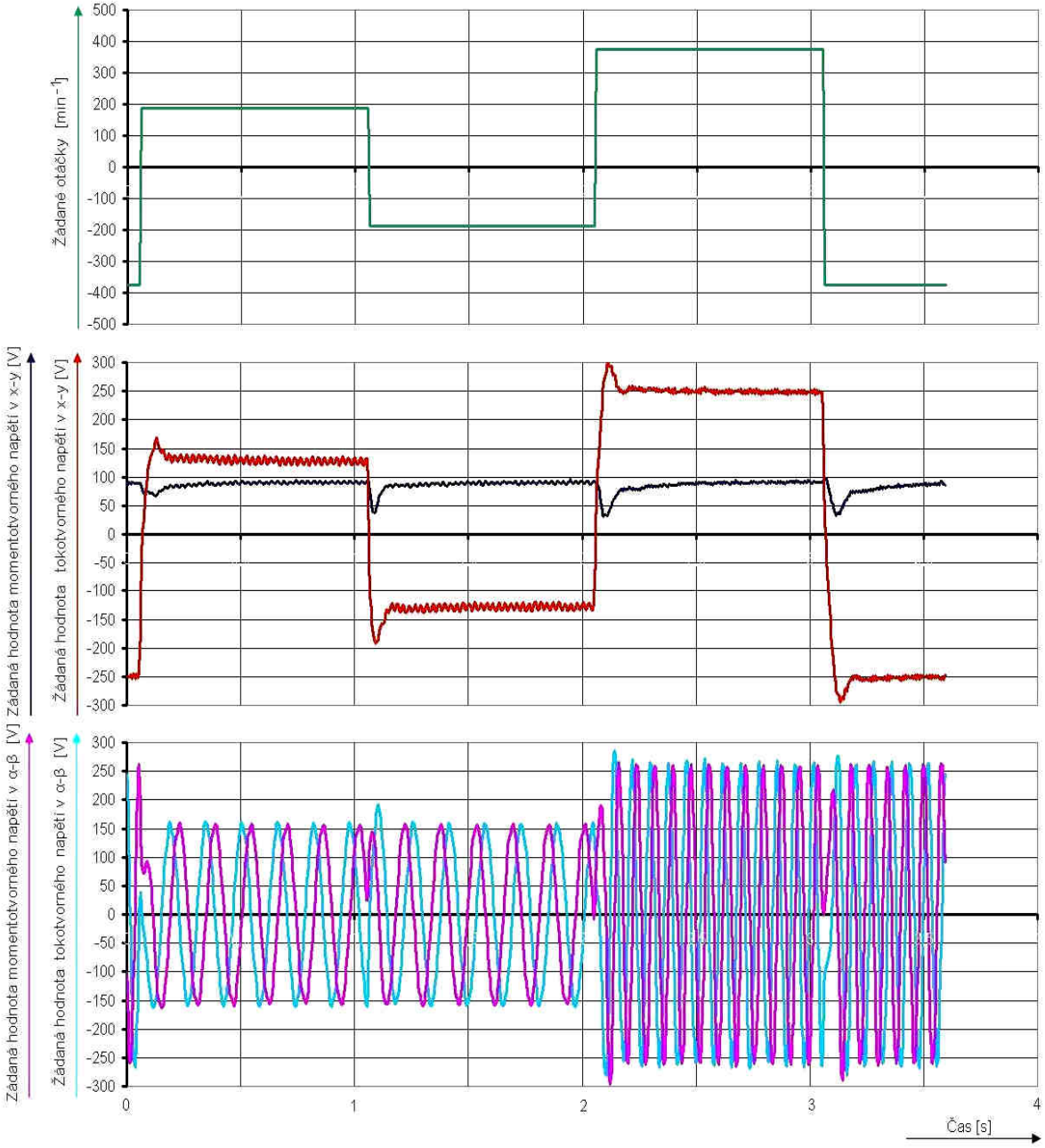
rec2.txt - Poznámkový blok

Soubor Úpravy Formát Zobrazení Nápověda

# Time [sec]	omega_req	Uxy.f16D	Uxy.f16Q	Ualfabetareq.f16Alpha	Ualfabetareq.f16Beta
0	-0.25	0.218414	-0.625671	0.611053	-0.256592
0.006	-0.25	0.219421	-0.624023	0.421906	-0.509369
0.012	-0.25	0.226318	-0.627014	0.154327	-0.648438
0.018	-0.25	0.220367	-0.617004	-0.164581	-0.634247
0.024	-0.25	0.227509	-0.632233	-0.441833	-0.506226
0.03	-0.25	0.224274	-0.613251	-0.606873	-0.241028
0.036	-0.25	0.224365	-0.632263	-0.667572	0.0675354
0.042	-0.25	0.223785	-0.612976	-0.550537	0.350464
0.048	-0.25	0.223419	-0.631256	-0.332642	0.581055
0.054	-0.25	0.224854	-0.613159	-0.0388184	0.651886
0.06	0.125	0.222931	-0.371979	0.098938	0.422272
0.066	0.125	0.210632	-0.116486	0.0268555	0.239166

Obrázek 8.31 Ukázka exportovaných dat z prostředí FreeMaster do souboru

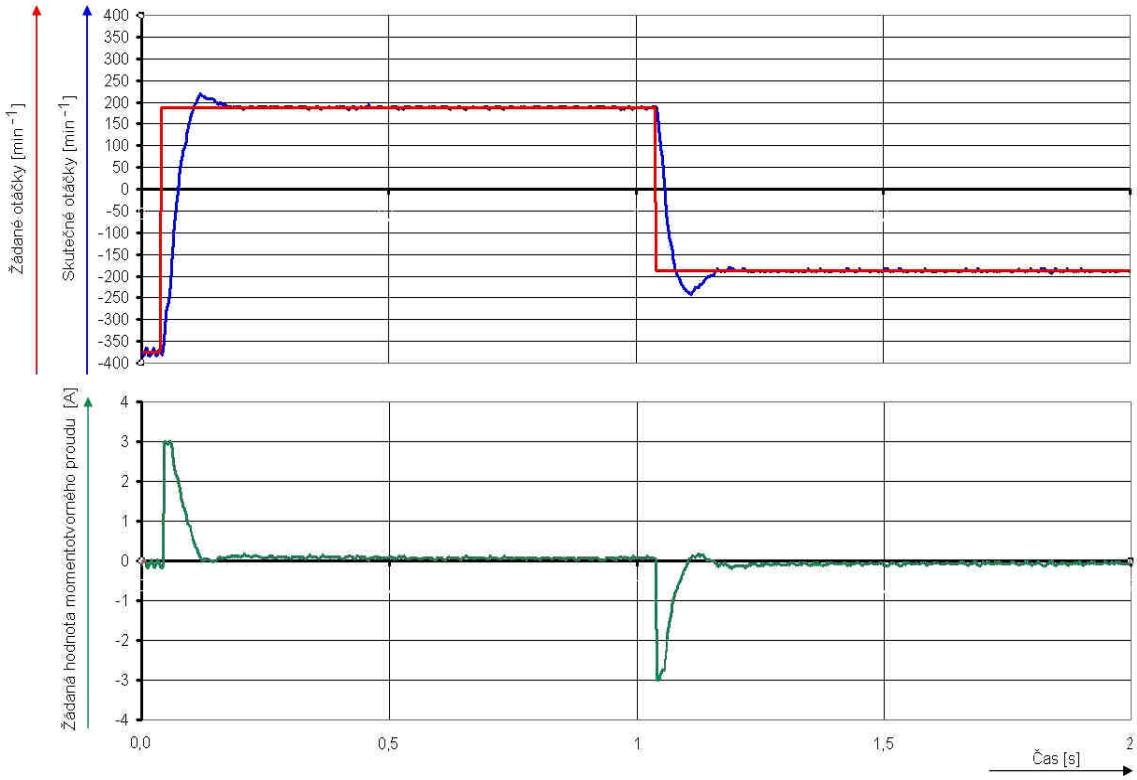
Na obrázku 8.32 jsou znázorněny průběhy závislostí exportované z textového souboru do programu Microsoft Excel, kde byly zpracovány a převedeny na grafy. Zelenou barvou je vyznačena závislost žádaných otáček v čase, červeně a modře jsou vykresleny časové závislosti tokotvorného a momentotvorného napětí v orientovaném souřadném systému (*x, y*) a bleděmodře a růžově jsou vykresleny časové závislosti tokotvorného a momentotvorného napětí v statorovém souřadném systému (*α, β*).



Obrázek 8.32 Zpracované průběhy

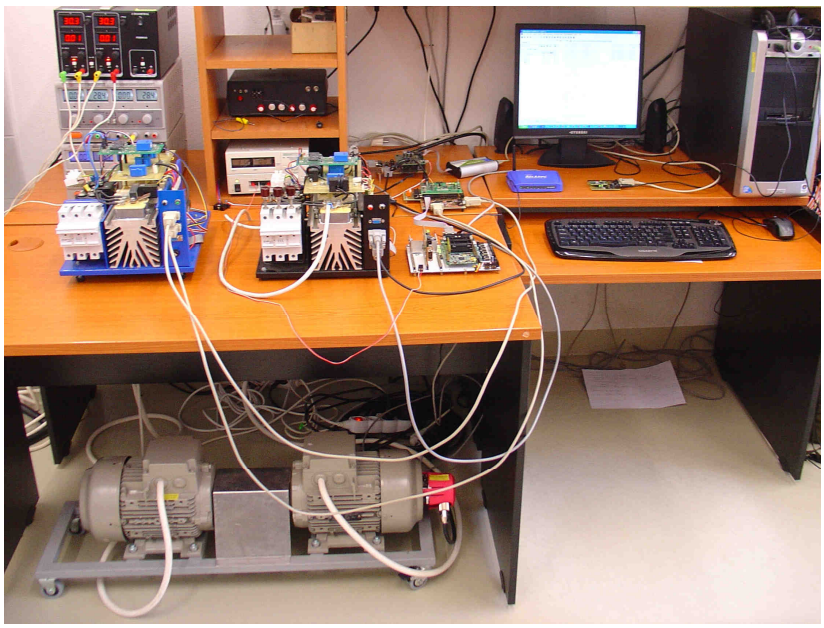
Následující obrázek 8.33 ukazuje vzájemnou časovou závislost mezi žádanými otáčkami vykreslenými červeně a skutečnými otáčkami vykreslenými modře. Pro doplnění je uvedena závislost momentotvorného proudu na čase.

Průběhy na obrázcích 8.32 a 8.33 reprezentují reverzaci nezatíženého asynchronního motoru, tedy situaci, kdy druhý motor sloužící k zatížení nebyl napájen.



Obrázek 8.33 Zpracované průběhy

Laboratorní pracoviště bezsenzorového řízení asynchronních motorů spolu WiFi přenosovou metodou SerialNET je znázorněno na obrázku 8.34. Infrastrukturní síť byla simulována vzájemně propojenými Access Pointy komunikujících mezi sebou lokální sítí (LAN).



Obrázek 8.34 Laboratorní pracoviště

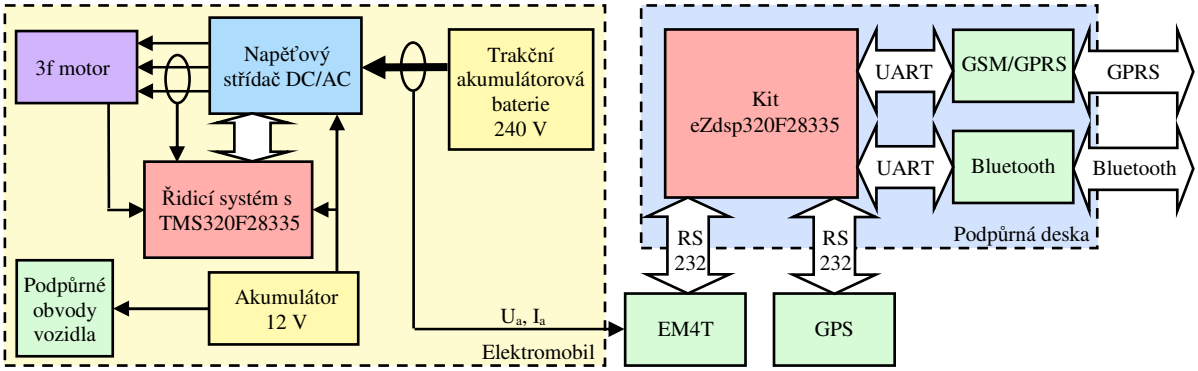
8.2.7 Monitorování spotřeby elektrické energie elektromobilu

Při vývoji a testování komponent pro vozidla s elektrickou trakcí jsou podstatné mimo jiné požadavky na napájecí management. Jelikož mohou být tato vozidla provozována různě daleko od vývojového pracoviště, je stěžejní zajistit přenos dat k centrále vzdáleného dohledu. Tyto data pak mohou nést informace o stavu jednotlivých komponent instalovaných ve vozidle, spotřebě elektrické energie, aktuální poloze, čase a podobně.

Jako trakční vozidlo byl použit elektromobil Tatra Beta znázorněný na obrázku 8.35, který byl sestaven na Katedře elektroniky, Vysoké školy báňské – Technické univerzity v Ostravě. Je napájen trakční olověnou akumulátorovou baterií PzB Hawker Perfekt Plus, čítající 120 článků s pancéřovými deskami. Kapacita této akumulátorové baterie činí 46 Ah, její jmenovité napětí je 240 V a hmotnost cca 500 kg. Elektromobil je poháněn vodou chlazeným třífázovým asynchronním motorem SIEMENS PV5105-4WS15-Z o jmenovitém výkonu 18 kW, jmenovitém proudu statoru 149 A, jmenovitém momentu 69 Nm. Maximální otáčky jsou 10000 min^{-1}. Napěťový střídač SIEMENS SIMOVERT 6SV1 je rovněž vodou chlazený a výkonová část je tvořena šesti IGBT tranzistory, maximální špičkový výstupní proud je 400 A a maximální výstupní napětí 220 V. Řízení střídače obstarává systém se signálovým procesorem TMS320F2812. Na obrázku 8.36 je zobrazena zjednodušená bloková struktura elektromobilu s připojeným elektroměrem EM4T a podpůrnou deskou, GPS přijímačem a přenosovými technologiemi GSM/GPRS a Bluetooth.

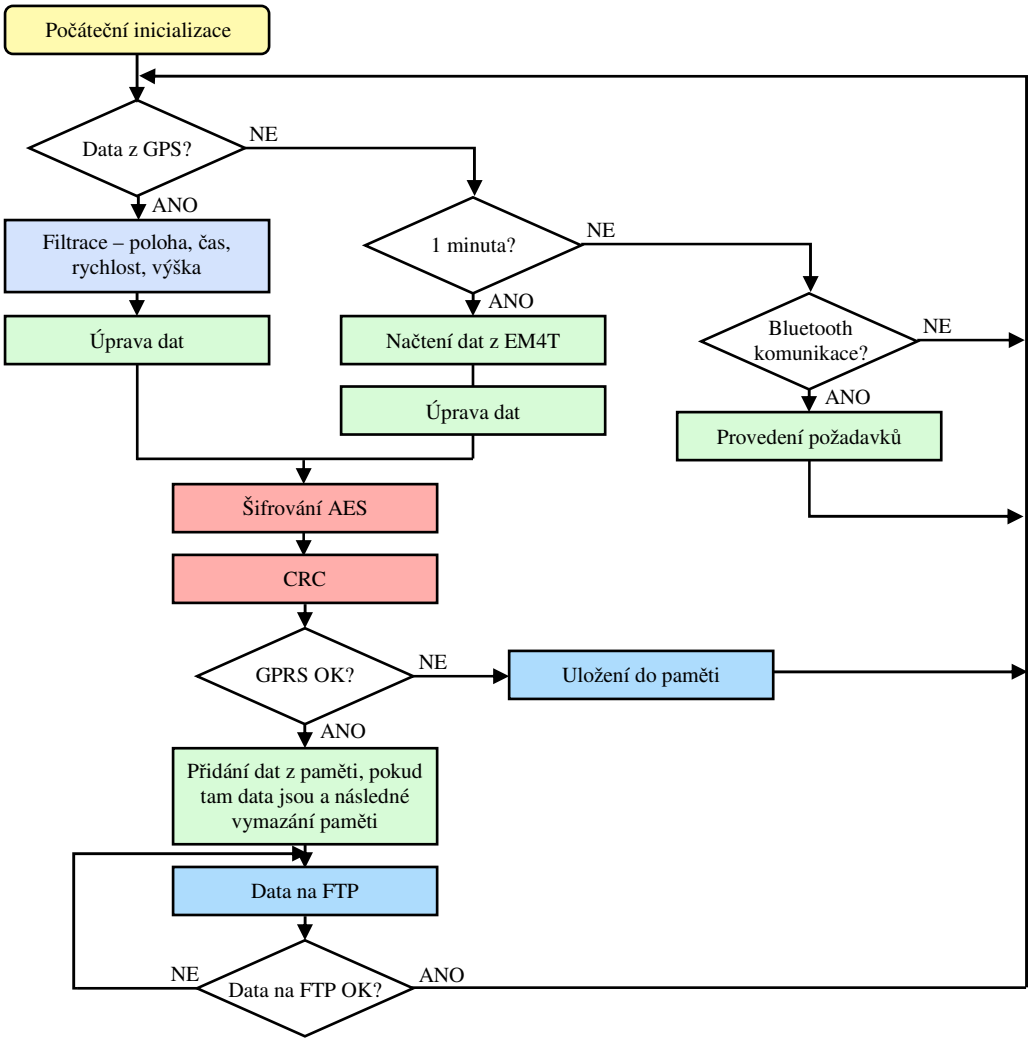
Obrázek 8.35 Elektromobil Tatra Beta

Je zřejmé, že kit eZdsp320F28335 osazený na podpůrné desce koordinuje datové toky mezi jednotlivými periferiemi. Přenosovou technologií GPRS jsou odesílána data na FTP server reprezentující spotřebovanou energii za každý minutový interval a dále informace o změnách polohy elektromobilu v tomto časovém intervalu s periodou každých 5 sekund. Bluetooth technologie slouží ke kontrolnímu bezdrátovému vyčtení údajů z paměti elektroměru v domovské stanici elektromobilu, případně pro budoucí nadstavbové funkce.



Obrázek 8.36 Zjednodušená bloková struktura elektromobilu a připojení systému pro přenos a zpracování dat

Na obrázku 8.37 je zobrazen zkrácený algoritmus programu. Po počáteční inicializaci, obsahující nastavení komunikace se všemi periferiemi, namapování paměťových prostorů a podobně, následuje čekací smyčka na jednotlivé události. Jedná se o čekání na data z GPS, které jsou k dispozici každých 5 sekund a testování minutového intervalu, po kterém budou vyčtena data z elektroměru EM4T. Také je testován požadavek na Bluetooth komunikaci.

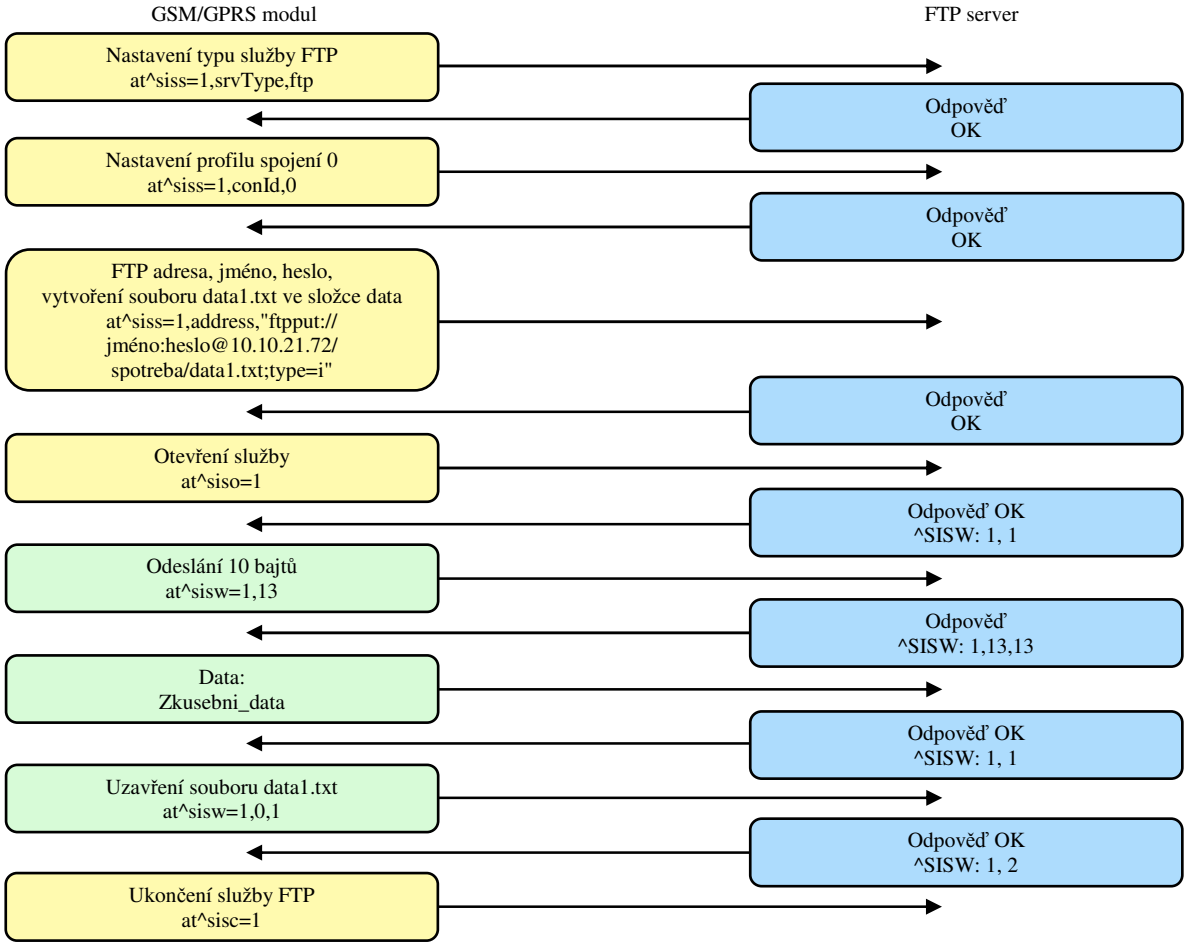


Obrázek 8.37 Algoritmus programu vyčítaní a odesílání dat

Jestliže jsou data z GPS k dispozici, následuje jejich filtrace a výběr požadovaných informací. Data se formálně upraví a zašifrují metodou AES, viz kapitola 4.1.1, kde je na obrázku 4.8 znázorněn také příklad šifrování šestnáctibajtového bloku dat. Po doplnění bloku dat CRC je otestováno GPRS připojení a pokud je vše v pořádku, následuje přenos dat na FTP server. V případě, že GPRS připojení není k dispozici, jsou data uložena do paměti a odeslána až po opětovném připojení spolu s následujícími daty. Pokud přenos proběhnul korektně, program se vrátí zpět k bodu za počáteční inicializací.

Když uplyne časový interval jedné minuty, je provedeno vyčtení dat z elektroměru EM4T, dle příkladu na obrázku 6.16. Data jsou opět formálně upravena a po zašifrování a doplnění CRC odeslána na FTP server.

Jakmile nastane v počáteční čekací smyčce potřeba Bluetooth komunikace je předpoklad, že elektromobil je v domovské stanici a mohou být prováděny další operace včetně rekonfigurace a vyčtení dat, která nebyla z důvodu možných problémů s GPRS spojením přenesena na FTP server.

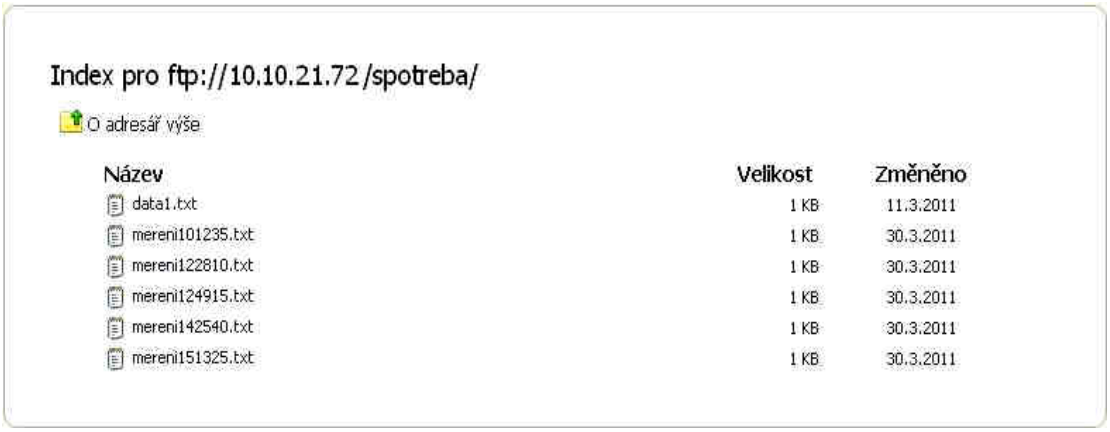


Obrázek 8.38 Komunikace mezi modulem MC55i a FTP serverem

Přenos dat na FTP server probíhá prostřednictvím GSM/GPRS sítě. Nejprve je provedena základní konfigurace modulu, nastavení přenosové rychlosti sériové komunikační linky (AT+IPR), deaktivace řízení toku (AT\Q0), nastavení GPRS spojení (AT^CGCONT),

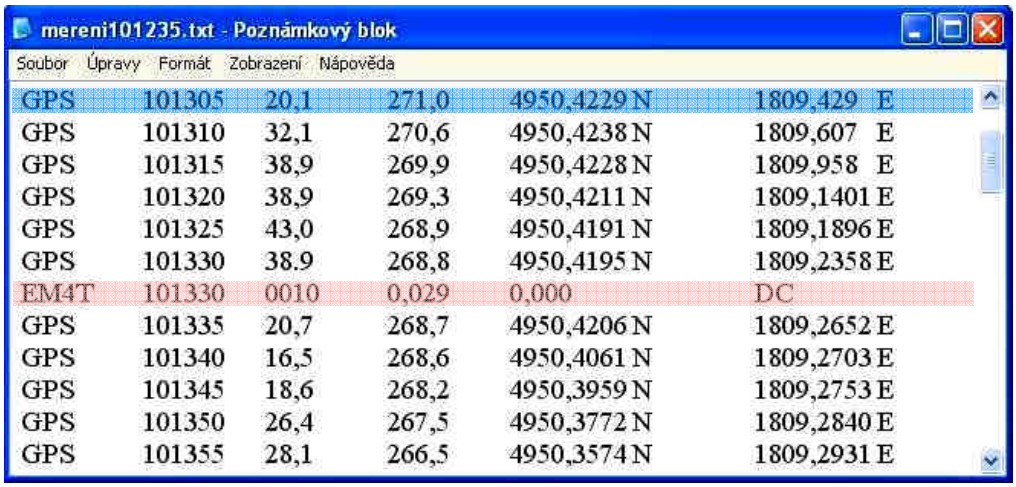
vytvoření GPRS spojení (ATD*99***1#) a podobně. Na obrázku 8.38 je znázorněn příklad testovací komunikace mezi kitem TMS320F28335 se signálovým procesorem, respektive GSM/GPRS modulem na rozšiřující desce a FTP serverem. FTP server má adresu ftp://10.10.21.72 a ve složce „spotreba“ bude vytvořen soubor „data1.txt“. Následně bude do souboru vložen text „Zkusebni_data“ a soubor uzavřen.

Finální formát odesílaných dat se liší od příkladu znázorněného na obrázku 8.38. Při každém měření je vytvořen soubor, do něhož jsou dopisována šifrovaná data reprezentující spotřebu elektrické energie a aktuální polohu. Na obrázku 8.39 je výřez z FTP serveru, na němž je vidět soubory z několika měření s názvem „mereni101235.txt“ až „mereni151325.txt“.



Obrázek 8.39 Výřez obrazovky FTP serveru

Výpis dešifrovaného a upraveného souboru „mereni101235.txt“ znázorňuje obrázek 8.40. Na řádcích uvozených „GPS“ jsou informace o čase, rychlosti, nadmořské výšce a poloze, kdežto na řádcích uvozených „EM4T“ jsou informace o čase a spotřebované elektrické energii. Blíže je specifikováno dekódování řádku uvozeného „GPS“ a „EM4T“ v tabulce 8.2 a 8.3.



Obrázek 8.40 Ukázka souboru „mereni101235.txt“

Tabulka 8.2 specifikuje modře označený řádek z obrázku 8.40 uvozený identifikátorem GPS. Údaje o zeměpisné šířce a zeměpisné délce jsou později využity k určení ujeté vzdálenosti, případně k zaznamenání polohy vozidla na mapě.

GPS	Identifikátor
101305	UTC čas ve formátu hhmmss (hodina – minuta – sekunda)
20,1	Aktuální rychlost v kilometrech za hodinu, 0000.0 až 1851.8 $km \cdot h^{-1}$
271,0	Nadmořská výška v metrech, -9999.9 až 99999.9 m
4950,4229	Zeměpisná šířka ve formátu ddmm,mmmm (stupně – minuty,desetinné vyjádření zbytku)
N	Určení polokoule u zeměpisné šířky (N – severní, S – jižní)
1809,429	Zeměpisná délka ve formátu dddmm,mmmm (stupně – minuty,desetinné vyjádření zbytku)
E	Určení polokoule u zeměpisné délky (E – východní, W – západní)

Tabulka 8.2 Dekódování řádku uvozeného „GPS“

Data z elektroměru EM4T, v obrázku 8.40 označené červeně, blíže popisuje tabulka 8.3. Jsou opět uvozena identifikátorem, za nímž následuje čas vyčtení z elektroměru, identifikátor události, kladná a záporná činná energie a typ napájecí soustavy.

EM4T	Správný směr vůči zemi, 000 až 359° (poprvé se pošlou nuly)
101330	UTC čas ve formátu hhmmss (hodina – minuta – sekunda)
0010	Identifikátor události viz tabulka 5.5
0,029	Kladná (potřebovaná) činná elektrická energie v kWh
0,000	Záporná (rekuperovaná) činná elektrická energie v kWh
DC	Typ napájecí soustavy

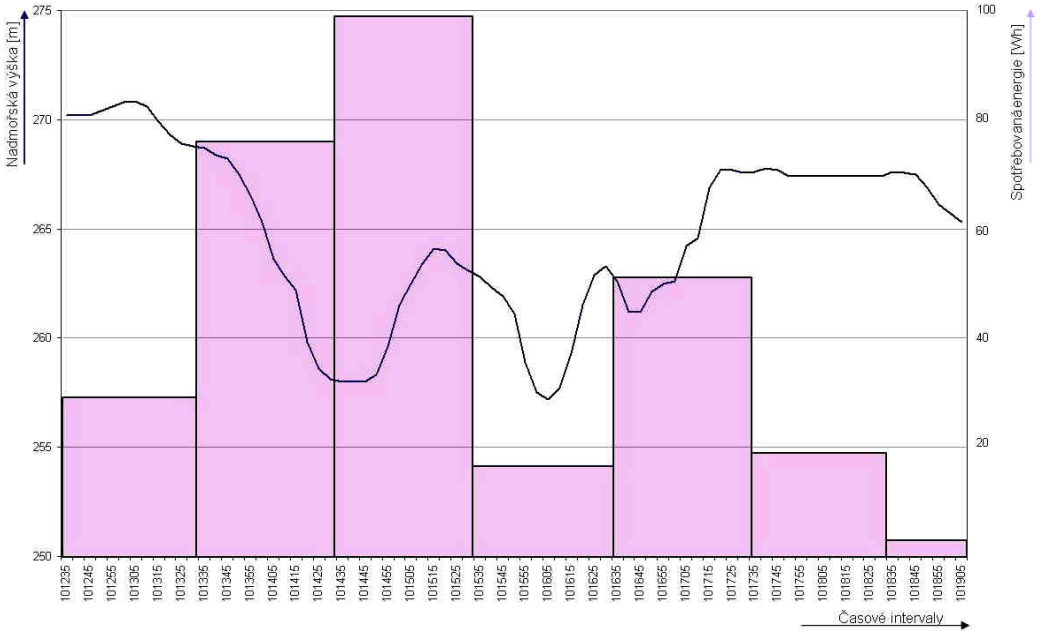
Tabulka 8.3 Dekódování řádku uvozeného „EM4T“

Byla provedena měření, na nichž byly ověřeny jak hardwarové bloky, tak i softwarové algoritmy. Obrázek 8.41 popisuje testovací trasu elektromobilu Tatra Beta. Start byl na parkovišti u budovy Vysoké školy báňské – Technické univerzity Ostrava, Krásnopolská 21/86 Ostrava – Pustkovec (značka A).

Obrázek 8.41 Ukázka testovací trasy

Trasa pokračovala ulicí Technologická, kde navázala na ulici Studentská. Po cca 1,6 km od startu následovalo odbočení na ulici Dr. Slabihoudka a trasa končila v areálu Vysoké školy báňské – Technické univerzity Ostrava, 17. listopadu 2171/15, před vjezdem mezi bloky E a F, znázorněno značkou B na obrázku 8.41. Celková ujetá vzdálenost byla cca 2,4 km.

Vyhodnocená data jsou znázorněna na následujících obrázcích. Obrázek 8.42 reprezentuje závislost dílčí spotřebované elektrické energie v jednotlivých časových intervalech na nadmořské výšce, respektive členitosti testovací trasy.

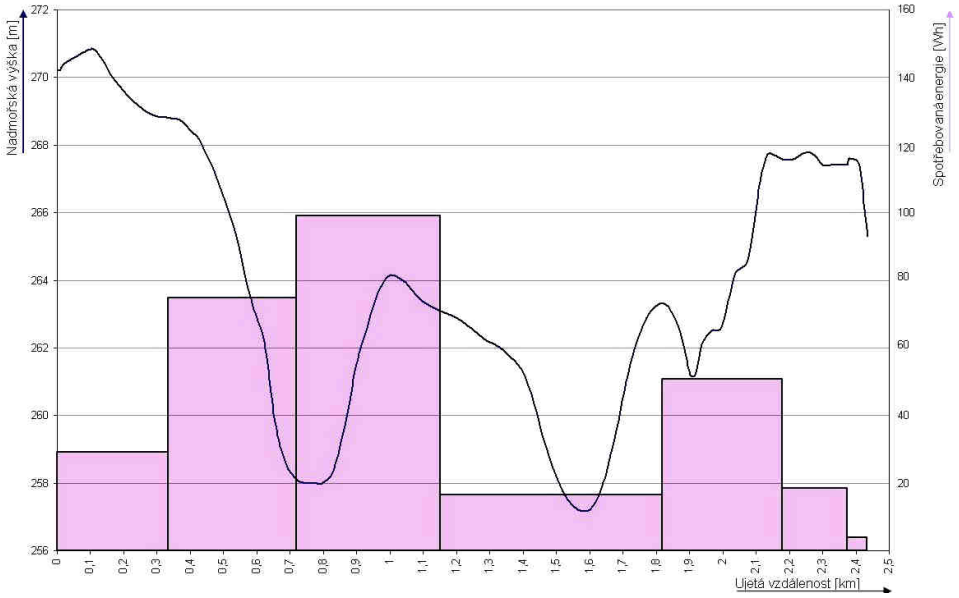


Obrázek 8.42 Závislost dílčí spotřebované energie v jednotlivých časových intervalech na členitosti testovací trasy

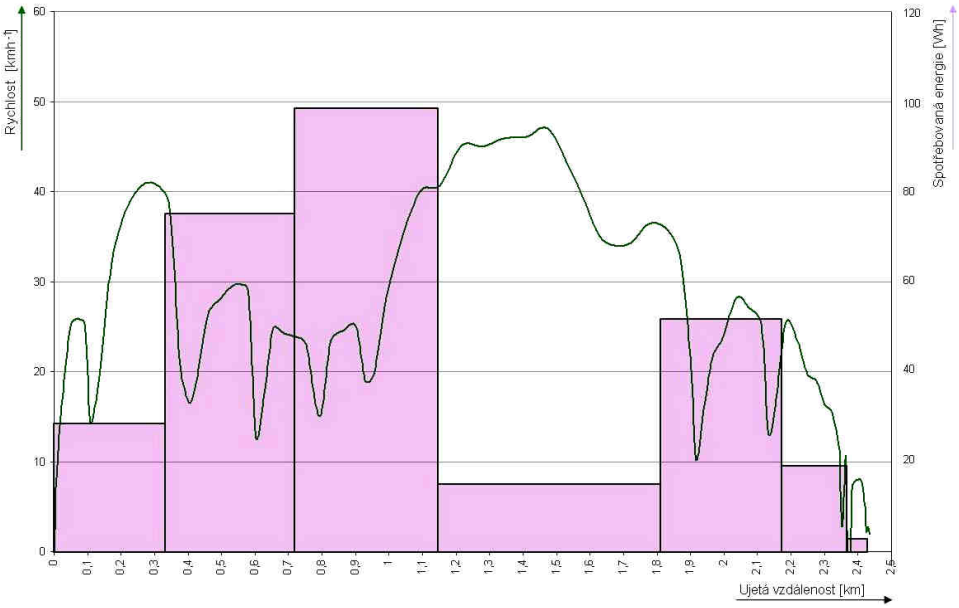
Obrázek 8.43 Závislost dílčí spotřebované energie v jednotlivých časových intervalech na rychlosti elektromobilu

Z obrázku 8.43 a 8.45 je zřejmé, že rychlost elektromobilu vcelku kolísala. Je to dáno častým výskytem retardérů na ulici Technologické a korekcích rychlosti elektromobilu při odbočování v jednotlivých křižovatkách. Obrázek 8.44 ukazuje závislost dílčí spotřebované energie na členitosti testovací trasy a ujeté vzdálenosti.

Ujetá vzdálenost byla vypočítána tak, že pomocí dostupného makra aplikace Microsoft Excel byly převedeny souřadnice polohy z WGS-84 na souřadnice UTM. UTM zobrazuje části elipsoidu do roviny a pak je možno vzdálenost dvou bodů počítat pomocí Pythagorovy věty, pokud tyto body leží ve stejné zóně.

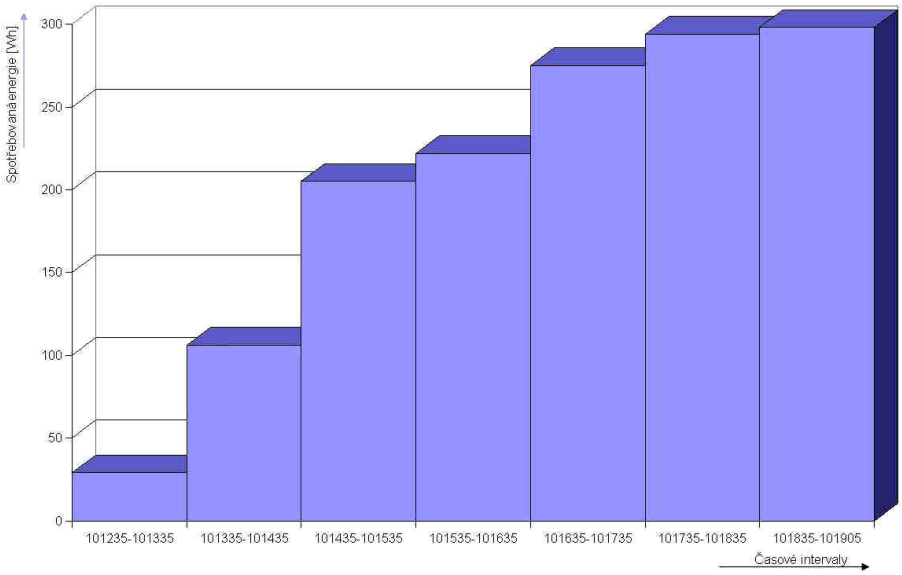


Obrázek 8.44 Závislost dílčí spotřebované energie na členitosti testovací trasy a ujeté vzdálenosti



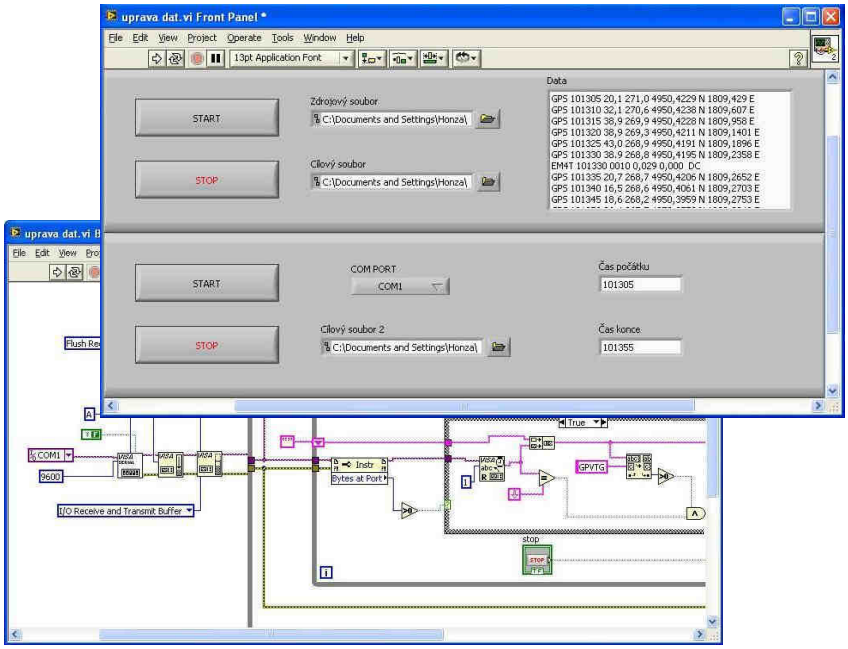
Obrázek 8.45 Závislost dílčí spotřebované energie na rychlosti elektromobilu a ujeté vzdálenosti

Celková spotřeba elektrické energie na testovací trase činila 298 Wh a průběh jejího nárůstu je znázorněn na obrázku 8.46, na rozdíl od předchozích grafů kdy byla prezentována dílčí spotřebovaná energie v jednotlivých intervalech.



Obrázek 8.46 Celková spotřebovaná elektrická energie

K vyčtení dat v domovské stanici prostřednictvím Bluetooth slouží ovládací program vytvořený v LabView, umožňující vyčtení informací o spotřebované elektrické energii z elektroměru EM4T a dešifrování dat uložených na pevném disku počítače. Experimentální verzi znázorňuje obrázek 8.47. Opět je emulována sériová Bluetooth linka použitím Seriál Port Profile. K dešifrování AES a kontrole CRC byly použity bloky dostupné v LabView, čímž se výrazně zjednodušil a zrychlil návrh softwarového prostředí.



Obrázek 8.47 Panel pro vyčtení a dešifrování dat z mobilního systému prostřednictvím Bluetooth

9 Přínosy

Tato práce přináší poznatky o bezdrátových přenosových metodách, podporovaných způsobech zabezpečení a možných rozšířeních. Jsou předvedeny možnosti využití jednotlivých přenosových technologií a ty také prakticky realizovány.

Přínosy:

- Shrnutí možností bezdrátového přenosu dat pomocí popsaných technologií, jejich zabezpečení proti zneužití a ukázání na možné nedostatky jednotlivých přenosových metod.
- Vývoj a realizace laboratorního pracoviště, které může být dále využito pro následné výzkumné a vývojové práce, případně pro výuku.
- Vývoj a implementace řídicích algoritmů pro moderní signálový procesor TMS320F28335 a také softwarových programů v podobě ovládacích nebo řídicích prostředí pro PC respektive Pocket PC.
- Aplikace zabezpečeného přenosu dat z technických zařízení, např. data ze střídavých regulovaných pohonů, data o spotřebě elektrické energie a údajů o poloze elektromobilu, respektive jiného trakčního vozidla.

Závěr

Práce se zabývá metodami přenosu a zabezpečení dat v mobilních aplikacích. Je zřejmé, že u mobilních systémů již kabelový přenos dat nesplní základní požadavky na flexibilitu a prostorové využití zařízení, nehledě na jejich technickou náročnost. Proto je práce zaměřena na aktuální bezdrátové přenosové technologie, jejich vlastnosti, zabezpečení proti zneužití přenášených dat a samozřejmě jejich aplikace.

Po úvodní části následuje kapitola seznamující se základními vlastnostmi použitých bezdrátových technologií. Jde konkrétně o mobilní technologii GPRS, která poskytuje vysoký stupeň mobility a je ji možno využít všude tam, kde je k dispozici GSM signál. Dále je popis věnován technologii WiFi, její struktuře a topologii Ad-hoc a infrastrukturních sítí. Poslední bezdrátovou technikou přenosu dat v první kapitole je masivně se rozvíjející technologie Bluetooth a tudíž je jí také věnována pozornost.

Samostatnou kapitolou je seznámení s globálním pozičním systémem neboli GPS. V práci je využíván pro určování nadmořské výšky, rychlosti a dalších údajů o poloze elektromobilu. Druhá kapitola tedy obsahuje základní informace o struktuře GPS, jednotlivých segmentech, použitých rádiových signálech, principech měření, určování polohy a standardech pro předávání dat.

V kapitole tři je věnována pozornost metodám detekce a odstraňování chyb při přenosu dat. Jsou zde uvedeny základní mechanismy odhalování chyb a podrobnější popis CRC. Tato metoda je dále využita při přenosu dat z elektromobilu. Rovněž jsou uvedeny možnosti, jakým způsobem chyby v přenosu po jejich detekci odstranit pomocí potvrzovacích mechanismů.

Zabezpečení proti zneužití informací je stále diskutovanějším problémem v systémech přenosu dat. Konkrétně rádiové sítě umožňují poměrně snadný odposlech pomocí směrových antén, i když tyto sítě nemusí mít velký výkon. Proto je u bezdrátových přenosových technologií kladen velký důraz právě na zajištění zabezpečeného přenosu dat. V kapitole čtyři je uvedeno základní rozdělení kryptografie, vědy zabývající se utajováním smyslu zpráv. Jsou ukázány výhody i nedostatky symetrických a asymetrických šifrovacích metod. Podrobněji je popsána symetrická iterační šifra AES s návazností na její praktickou implementaci do systému s DSC TMS320F28335 a do obslužného programu určeného k dešifrování přenesených dat. Dále jsou v kapitole pět shrnuty metody využívané pro zabezpečení u jednotlivých v práci použitých bezdrátových přenosových metod.

Laboratorní pracoviště k ověření komunikace s jednotlivými přenosovými technologiemi a dalšími hardwarovými bloky, včetně GPS přijímače a trakčního elektroměru EM4T, které jsou využity pro monitoring spotřeby energie a polohy elektromobilu, je popsáno v kapitole šest. Je proveden rozbor požadavků na mobilní přenosový systém, který je následně navržen. Skládá se z podpůrné desky obsahující napájecí management a osazený kit s DSC

TMS320F28335. Do této podpůrné desky jsou následně dle potřeb osazovány jednotlivé rozšiřující desky s bezdrátovými technologiemi GSM/GPRS, WiFi, případně Bluetooth. Veškeré navržené a hotové hardwarové moduly jsou popsány v této kapitole, dále jsou zde znázorněny blokové struktury a možnosti využití těchto modulů. Následně jsou v kapitole sedm stručně popsána softwarová prostředí umožňující programování DSC, tvorbu uživatelského prostředí na PC a také komunikaci a nastavení jednotlivých hardwarových bloků.

Stěžejní částí práce jsou experimentální výsledky, při nichž došlo nejen k ověření nezabezpečeného, ale i zabezpečeného přenosu dat z mobilního systému prostřednictvím dříve popsaných bezdrátových přenosových technologií do centrálního počítače. U technologie Bluetooth byla data přenášena mezi mobilním systémem a personálním počítačem, případně Pocket PC s operačním systémem Windows Mobile 6.5. Samozřejmostí bylo vytvoření obslužných aplikací pro PC i pro Pocket PC. Technologie WiFi poskytla více aplikačních možností v podobě přenosu předzpracovaných dat na FTP server, případně vytvoření asynchronního datového tunelu v Ad-hoc nebo infrastrukturní topologii. Konkrétně infrastrukturního asynchronního přenosu bylo využito pro transfer dat mezi pracovištěm pro bezsenzorové řízení asynchronních motorů a ovládacím programem FreeMaster. Nechybí ani aplikace v podobě odesílání SMS na určené telefonní číslo při splnění předem daných podmínek. Podstatnou aplikaci představuje monitorování spotřeby elektrické energie elektromobilu, včetně přenosu informací o aktuální poloze, rychlosti, nebo nadmořské výšce. Data byla zabezpečena metodou AES a dále odesílána prostřednictvím GPRS na FTP server a následně s pomocí vytvořené aplikace dešifrována a zpracována do přehledných grafů.

Na základě dosažených výsledků je možno říci, že stanovené dílčí cíle byly v plném rozsahu splněny. Značné množství získaných poznatků a vědomostí v oblastech bezdrátového přenosu dat a jejich zabezpečení je prémií za některá úskalí, vznikající zejména při realizaci, která se podařilo zdárně vyřešit. Na práci lze volně navázat, případně může sloužit pro další oblast výzkumu, nebo výuky na Katedře elektroniky.

Použitá literatura

[1] Hanus, S. *Bezdrátové a mobilní komunikace*. Vysoké učení technické v Brně, ISBN 80-214-1833-8.

[2] Heine, G. *GPRS from A-Z*. Boston, Artech House, 2001, 268 s. ISBN 1-58053-181-4.

[3] Seure, E., Saveli, P., Pietri, P.J. *GPRS for Mobile Internet*. Boston, Artech House, 2003, 419 s. ISBN 1-58053-600-X.

[4] *Wi-Fi* [online]. 2008 [cit. 2010-01-05]. Wi-Fi Wireless LAN. Dostupné z WWW: <http://wi-fi.unas.cz/>.

[5] *Wapedia* [online]. 2009, 2009-12-11 [cit. 2010-01-07]. WiFi. Dostupné z WWW: <http://wapedia.mobi/cs/Wi-Fi>.

[6] Bartáček, J. *Stránky o elektronice a počítačích* [online]. 2009 [cit. 2010-04-12]. Bezdrátové sítě. Dostupné z WWW: <http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite>.

[7] *Novinky na Internetu* [online]. 2009 [cit. 2010-04-12]. WiFi. Dostupné z WWW: <http://novinky.enachod.cz/wifi/>.

[8] Zandl, P. *Bezdrátové sítě WiFi*, Computer Press ISBN 80-7226-632-2.

[9] Popek, R. *Inteligentní bezdrátové komunikační subsystémy*. Ostrava, 2009, 27 s. Semestrální práce. VŠB – Technická Univerzita Ostrava.

[10] *PCWorld* [online]. 2009 [cit. 2010-05-28]. Základy technologie Bluetooth: původ a rozsah funkcí. Dostupné z WWW: <http://pcworld.cz/hardware/Zaklady-technologie-Bluetooth-puvod-a-rozsah-funkci-6635>.

[11] Morrow, R. *Bluetooth Operation and Use*. New York, McGraw-Hill, 2002, 567 s. ISBN 0-07-138779-X.

[12] Tkáč, J. *Jak na Bluetooth v rekordním čase*. Praha, Grada Publishing, 2005, 84 s. ISBN 80-247-1081-1.

[13] Prokopec, J., Hanus, S. *Systémy mobilních komunikací.* Vysoké učení technické v Brně.

[14] Rapant, P. *Družicové polohové systémy.* Ostrava, VŠB – TU Ostrava, 2002, 197 s. ISBN 80-248-0124-8.

[15] Ackroyd, N.,Lorimer, R. *Global Navigation. A GPS User's Guide. Second Edition.* London, Lloyd's of London Press, 1994, 196 s. ISBN 978-1-85044-517-3.

[16] Steiner, I., Černý, J. *GPS od A do Z*. 4. vyd. Praha: eNav, 2006, ISBN 80-239-7516-1.

[17] White, C. M., *Data Communicatins & Computer Networks. Third Edition.* Boston, Course Technology, 2004, 520 s. ISBN 0-619-16035-7.

[18] Peterka, J. *eArchiv.cz* [online]. 2009 [cit. 2011-03-03]. Základní formy přenosů. Dostupné z WWW: <http://www.earchiv.cz/a91/a140c110.php3>.

[19] Peterka, J. *eArchiv.cz* [online]. 2008 [cit. 2011-01-07]. Zajištění spolehlivosti. Dostupné z WWW: <http://www.earchiv.cz/b05/b1200001.php3>.

[20] Marx, Z. *Bezpečnostní rozhraní mezi informačními systémy*. Praha, 2009, 73 s. Bakalářská práce. Bankovní institut vysoká škola Praha.

[21] Stallings, W. *Cryptography and Network Security*. United States of America: Pearson Education, Inc., 2006, 680 s. ISBN 0-13-187316-4.

[22] Pužmanová, R. *Bezpečnost bezdrátové komunikace*. Brno: CP Books, a.s, 2005, 680 s. ISBN 80-251-0791-4.

[23] Matoušek, R. *Metody kódování.* Brno, VUT v Brně, 2006, 88 s.

[24] Katz, J. *Introduction to modern cryptography.* Boca Raton, Chapman & Hall/CRC, 2008. 534 s. ISBN 978-1-58488-551-1.

[25] Maliník, M. *Základy praktické kryptografie* [online]. Zlín: 2009. 36 s. Prezentace. UTB Zlín, FAI. Dostupné z WWW: <www.vyuka.fai.utb.cz>.

[26] Stanek, M. *Základy kryptológie* [online]. 2004 [cit. 2011-03-01]. Dostupné z WWW: <http://www.dcs.fmph.uniba.sk/~stanek/crypto/main2.pdf>.

[27] *Advanced Encryption Standard*. National Institute of Standards and Technology, 2001. 47 s. Dostupné z WWW: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[28] Wagner, N. R. *University of Texas at San Antonio* [online]. 2002 [cit. 2011-01-08]. The Laws of Cryptography: Test Runs of the AES Algorithm. Dostupné z WWW: <http://www.cs.utsa.edu/~wagner/laws/AEStestRuns.html>.

[29] Brzek, T. *Zabezpečení wi-fi sítí, Wi-fi network security*. Most, 2008, 40 s. Bakalářská práce. ČZU Praha.

[30] *Texas Instruments* [online]. 1995 [cit. 2010-02-13]. Dostupné z WWW: <http://www.ti.com/>.

[31] *ConnectBlue* [online]. 2010 [cit. 2011-02-15]. OEM RS232 Module Adapter 3. Dostupné z WWW: <http://www.connectblue.com/products/wireless-accessories/wireless-adapter-boards-kits/oem-rs232-module-adapter-3/>.

[32] *Spezial Elektronics* [online]. 1999 [cit. 2010-02-16]. OEM Serial Port Adapter™. Dostupné z WWW: <http://www.spezial.cz/pdf/em_ds_oemspa_312_332.pdf>.

[33] *Spezial Elektronics* [online]. 1999 [cit. 2010-02-21]. Nano Socket iWiFi™. Dostupné z WWW: <http://www.spezial.cz/pdf/Nano_Socket_iWiFi_DS.pdf>.

[34] *Citerion* [online]. 2011 [cit. 2010-11-07]. MC55i. Dostupné z WWW: <http://www.cinterion.com/mc55i.html>.

[35] *Garmin* [online]. 2010 [cit. 2011-01-09]. Manuals for GPS 16™. Dostupné z WWW: <https://buy.garmin.com/support/manuals/manuals.htm?partNo=010-00258-53>.

[36] LEM. *Electronic Energy Meter EM4T: User manual.* Švýcarsko, 2006.

[37] Žídek, J. *Uživatelský manuál k LabVIEW 7.1*. VŠB-TU Ostrava, 2006, Katedra elektrických měření.

[38] Johnson, G.W. *LabVIEW Graphical Programming: Practical Applications in Instrumentation and Control*. New York, McGraw-Hill, 1994, 522 s. ISBN 0-07-032692-4.

[39] ConnectBlue. *SPA Toolbox User Manual.* Sweden, 2010.

[40] ConnectOne. *iChip Config Utility User Manual.* Israel, 2009.

[41] ConnectOne. *iChip FTP Client Theory of Operation.*Israel, 2009.

[42] ConnectOne. *SerialNET Theory of Operation.* San Jose, 2002.

[43] Rech, P. *Bezsenzorové řízení střídavého regulovaného pohonu se synchronním motorem s permanentními magnety.* VŠB-TU Ostrava, 2010, 92 s.

[44] Škopek, M. *Systémy měření spotřeby elektrické energie trakčních vozidel.* VŠB-TU Ostrava, 2009, 93 s.

[45] Racek, S. *Objektově orientované programování v C++*. České Budějovice: Kopp, 1994, ISBN 80-85828-20-0.

[46] Dostálek, L. *Velký průvodce protokoly TCP/IP: Bezpečnost*. Praha, Computer Press, 2003, 572 s. ISBN 80-7226-849-X.

[47] Mielczarek, W. *Szeregowe interfejsy cyfrowe.* Gliwice, Helion, 1993, 162 s. ISBN 83-85701-23-0.

Publikace autora

[I.] Michalík, J., Dostalík, M., Vaněk, J.: Mikroprocesorový systém pro aplikace výkonové elektroniky. In *Časopis pre elektrotechniku a energetiku, Elosys 2008*, 2008, vol. 14., s. 106-109.

[II.] Vaněk, J., Michalík, J., Dostalík, M.: Řídicí mikropočítačový systém s DSP TMS320F28335 pro aplikace v průmyslové elektronice. In *Časopis pre elektrotechniku a energetiku, ELOSYS 2008*, 2008, vol. 14., s. 102-105.

[III.] Vaněk, J., Michalík, J.: Řídící mikropočítačový systém s DSP TMS320F28335 . In *XXII. Mezinárodné sympózium učiteľov elektrických pohonov, SYMEP 2008*. Trenčín: Trenčianska univerzita Alexandra Dubčeka v Trenčíne v spolupráci s Mechatronik, n.o. , 2008, vol. 22., 65-67, ISBN 978-80-8075-337-5.

[IV.] Vaněk, J., Michalík, J.: Universal control system with DSC TMS320F28335. In *Workshop of Faculty of Electrical Engineering and Computer Science, WOFEX 2008*, Ostrava: VŠB-TUO, 2008, vol. 6th, p. 182-186, ISBN 978-80-248-1807-8.

[V.] Michalík, J., Vaněk, J.: Laboratory Workplace for Teaching of Communication Technologies of Microcomputer Systems. In *Workshop of Faculty of Electrical Engineering and Computer Science, WOFEX 2009*, Ostrava: VŠB-TU Ostrava, 2009, vol. 7th, p. 136-141, ISBN 978-80-248-2028-6.

[VI.] Vaněk, J.: Support Board for Microcomputer Control System withTMS320F28335. In *Workshop of Faculty of Electrical Engineering and Computer Science, WOFEX 2009*. VŠB - Technical University of Ostrava, 2009, 153-157, ISBN 978-80-248-2028-6.

[VII.] Pumr, J., Michalík, J., Hudeček, P., Sobek, M., Vaněk, J.: Aplikace řídících systémů s DSC, Rožnov pod Radhoštem: In *Sborník přednášek Perspektivy elektrotechniky 2009,* Střední škola informatiky, elektrotechniky a řemesel, 2009, ISBN 978-80-254-4052-0.

[VIII.] Vaněk, J., Michalík, J.: Aplikované neuronové sítě pro zpracování číslicových signálů s DSC TMS320F28335. In *IEEE Workshop Králíky 2009.* Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, s. 184-187, ISBN 978-80-214-3938-2.

[IX.] Vaněk, J., Škopek, M.: Monitorovací systém pro měření spotřeby energie trakčních vozidel. In *XLI. sešit Katedry elektrotechniky,* Ostrava: VŠB - Technická univerzita Ostrava, 2009, s. 38-42, ISBN 978-80-248-2020-0.

Publikace, které jsou nebo budou uvedeny na Web of Science (*http://www.webofknowledge.com*).

[X.] Brandštetter P., Michalík J, Pumr J., Vaněk J.: Microcomputer Control System for Industrial Electronics Applications. In *International Conference Applied Electronics,* Pilsen, Czech Republic, 2009, pp. 57 – 60, ISBN 978-80-7043-781-0

[XI.] Brandstetter P., Michalik J., Vanek J.: Workplace for Measurement of Selected Parameters of Communication Buses. In *International Conference Applied Electronics,* Pilsen, Czech Republic, pp. 47-50, 2010, ISBN 978-80-7043-865-7.

[XII.] Brandstetter P., Chlebis P., Michalik J., Vanek J.: System for Monitoring and Data Transmission from Mobile Devices. In *International Conference on Signals and Electronic Systems - ICSES´10*, Gliwice, Poland, pp. 363-366, 2010, ISBN 978-1-4244-5307-8.

Řešené grantové projekty

- IGA 9/2008 - Systémy pro bezdrátovou komunikaci a přenos dat z mobilních mechatronických systémů, projekt Interní grantové agentury FEI VŠB-TU Ostrava, člen řešitelského týmu v roce 2008.
- IGA 10/2008 - Výzkum výkonových LED jako zdrojů pro optickou komunikaci mezi pohybujícími se vozidly, projekt Interní grantové agentury FEI VŠB-TU Ostrava, člen řešitelského týmu v roce 2008.
- IGA 9/2009 - Bezdrátový přenos provozních parametrů trakčních vozidel, projekt Interní grantové agentury FEI VŠB-TU Ostrava, člen řešitelského týmu v roce 2009.
- FRVŠ 150/2009/G1 - Laboratorní pracoviště pro výuku komunikačních technologií mikropočítačových systémů, projekt Fondu rozvoje vysokých škol, řešitel v roce 2009.
- SP/201098 - Moderní řídicí algoritmy mechatronických systémů s elektrickými regulovanými pohony, projekt SGS VŠB-TU Ostrava, člen řešitelského týmu v roce 2010.